PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001 PADA KOMISI PEMILIHAN UMUM (KPU) PROVINSI JAMBI

Astrid Rhamadina.H[1], M.Yusuf[2], Bastomi Baharsyah[3]
astridrmdhn@gmail.com[1], yusufyssc@uinjambi.ac.id[2], bastomibaharsyah@uinjambi.ac.id[3]
UIN Sulthan Thaha Saifuddin Jambi

ABSTRAK

Keamanan informasi merupakan pilar fundamental dalam mendukung kelangsungan tata kelola pemerintahan yang baik, terlebih bagi lembaga negara seperti Komisi Pemilihan Umum (KPU) yang berperan strategis dalam penyelenggaraan pemilu. KPU Provinsi Jambi sebagai penyelenggara pemilu di tingkat daerah menghadapi tantangan signifikan dalam mengelola dan melindungi informasi penting, terutama di tengah meningkatnya intensitas serta kompleksitas ancaman siber. Penelitian ini dilatarbelakangi oleh kebutuhan mendesak untuk menerapkan sistem pengamanan informasi yang sistematis, terstruktur, dan sesuai dengan standar internasional, dalam hal ini ISO/IEC 27001. Penelitian ini bertujuan untuk merancang sistem manajemen keamanan informasi (SMKI) berbasis ISO/IEC 27001 sebagai upaya mitigasi risiko dan peningkatan ketahanan informasi di lingkungan KPU Provinsi Jambi. Pendekatan yang digunakan adalah kualitatif dengan metode pengumpulan data berupa observasi langsung, wawancara mendalam dengan pemangku kepentingan terkait, serta analisis risiko terhadap sistem informasi yang berjalan. Temuan dari hasil penelitian menunjukkan bahwa KPU Provinsi Jambi telah menerapkan sebagian elemen keamanan informasi melalui Sistem Pemerintahan Berbasis Elektronik (SPBE), namun belum memiliki kerangka kebijakan formal dan menyeluruh yang mengacu pada ISO/IEC 27001. Terdapat pula keterbatasan dari aspek infrastruktur teknologi, kapasitas sumber daya manusia, dan dokumentasi kontrol keamanan yang berdampak pada efektivitas perlindungan informasi. Sebagai solusi strategis, penelitian ini menghasilkan rancangan dokumen awal kebijakan keamanan informasi yang disusun berdasarkan klausul inti ISO/IEC 27001. Dokumen tersebut mencakup ruang lingkup organisasi, identifikasi isu internal dan eksternal melalui analisis PESTLE, analisis risiko terhadap aset informasi, serta penetapan peran dan tanggung jawab terkait pengelolaan keamanan informasi. Penyusunan dilakukan dengan pendekatan Plan-Do-Check-Act (PDCA) untuk memastikan keberlanjutan pengelolaan keamanan. Rekomendasi lanjutan mencakup pelatihan internal pegawai, peningkatan infrastruktur teknologi informasi, serta penerapan audit dan review berkala guna menjaga kesesuaian sistem dengan dinamika ancaman terkini. Melalui implementasi ISO/IEC 27001 secara bertahap dan berkelanjutan, KPU Provinsi Jambi diharapkan mampu meningkatkan kapabilitas dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi, sekaligus membangun kepercayaan publik terhadap transparansi dan akuntabilitas proses pemilu. Penelitian ini memberikan kontribusi praktis bagi lembaga pemerintah dalam mengadopsi standar keamanan informasi global dalam konteks lokal.

Kata Kunci: Keamanan Informasi, ISO/IEC 27001, KPU, Manajemen Risiko, Standar Keamanan, SPBE.

ABSTRACT

Information security is a fundamental pillar in supporting the sustainability of good governance, particularly for state institutions such as the General Election Commission (KPU), which holds a strategic role in organizing democratic elections. The KPU of Jambi Province, as the regional electoral authority, faces significant challenges in managing and protecting sensitive information, especially amid the growing intensity and complexity of cyber threats. This study is motivated by the urgent need to implement a systematic, structured, and internationally recognized information security framework—namely ISO/IEC 27001. The objective of this research is to design an

Information Security Management System (ISMS) based on ISO/IEC 27001 as a risk mitigation strategy and to enhance information resilience within the KPU of Jambi Province. A qualitative approach was employed, utilizing data collection methods such as direct observation, in-depth interviews with relevant stakeholders, and risk analysis of the existing information system. The findings indicate that while the KPU of Jambi Province has implemented certain elements of information security through the Electronic-Based Government System (SPBE), it still lacks a formal and comprehensive policy framework aligned with ISO/IEC 27001. Limitations were also identified in terms of technological infrastructure, human resource capacity, and security control documentation, which collectively affect the effectiveness of information protection efforts. As a strategic solution, this study produced a draft of an initial information security policy document based on the core clauses of ISO/IEC 27001. The document includes organizational scope, identification of internal and external issues through a PESTLE analysis, risk assessment of information assets, and a clear definition of roles and responsibilities in managing information security. The policy design follows the Plan-Do-Check-Act (PDCA) model to ensure sustainability in its implementation. Additional recommendations include employee training, enhancement of IT infrastructure, and the adoption of regular audits and reviews to maintain system relevance in the face of evolving threats. Through the gradual and continuous implementation of ISO/IEC 27001, the KPU of Jambi Province is expected to strengthen its capability to safeguard the confidentiality, integrity, and availability of information, while simultaneously building public trust in the transparency and accountability of the electoral process. This study offers practical contributions for government institutions in adopting global information security standards within a localized operational context.
Keywords: ISO/IEC 27001, Information Security Management, KPU Jambi Province, SPBE.

PENDAHULUAN

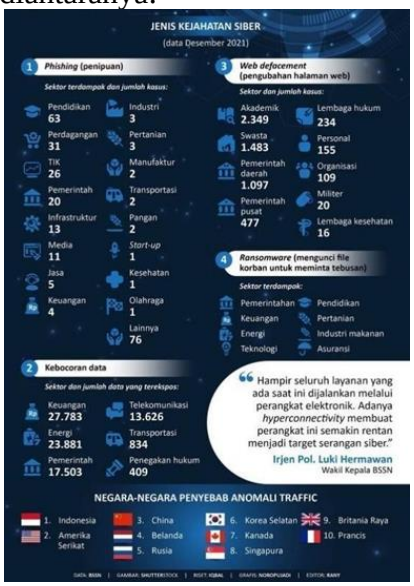
Komisi Pemilihan Umum (KPU) merupakan salah satu lembaga yang memanfaatkan teknologi informasi, seperti platform digital berbasis web dan aplikasi, untuk mendukung transparansi, efisiensi, serta kemudahan akses dalam pelaksanaan pemilu, termasuk dalam hal pengelolaan data pemilih, rekapitulasi hasil suara, dan distribusi informasi kepada publik. Namun, perkembangan teknologi informasi juga membawa tantangan, terutama dengan maraknya penyalahgunaan oleh pihak-pihak tidak bertanggung jawab, yang menimbulkan risiko dan ancaman dalam penggunaannya. Salah satu bentuk ancaman yang menjadi tantangan besar adalah kejahatan siber yang mengacu pada media elektronik dalam jaringan komputer yang digunakan sebagai sarana komunikasi, baik satu arah maupun dua arah, dengan interaksi online (Techterms, 2022). Ancaman ini dapat berdampak langsung terhadap kerahasiaan, integritas, dan ketersediaan data pemilu yang sangat krusial.

Global Risks Landscape Report melalui surveinya pada tahun 2017 dan 2018 menempatkan serangan siber (cyberattacks) dengan prioritas tertinggi dibandingkan dengan interstate conflict ataupun serangan teroris. Serangan siber sendiri memiliki berbagai bentuk seperti Cyber War, Cyber Terrorism, Cyber Espionage dan Cyber Crime. Ancaman-ancaman tersebut merupakan salah satu bentuk ancaman non-tradisional dan menjadi suatu isu yang tersekuritisasi karena mengancam eksistensi dan keamanan negara sebagai referen tertinggi yang mencakup keamanan militer, lingkungan, ekonomi, sosial dan politik.

Kondisi ini menjadi perhatian khusus bagi KPU Provinsi Jambi yang berperan menyelenggarakan pemilu di tingkat daerah. Selama ini, sistem informasi yang digunakan oleh KPU Provinsi Jambi belum sepenuhnya dirancang dengan mengacu pada standar keamanan informasi yang terstruktur dan menyeluruh. Di tengah meningkatnya kasus kejahatan siber, terutama yang menyasar institusi pemerintahan, KPU Provinsi Jambi memerlukan sistem pengamanan yang mampu melindungi aset informasi dari potensi serangan digital maupun gangguan teknis.

Komisi Pemilihan Umum (KPU) Provinsi Jambi sebagai penyelenggara pemilihan umum di Indonesia seharusnya dapat belajar dari pengalaman beberapa negara dalam pengamanan pemilu. Saat ini KPU Provinsi Jambi lebih tertantang lagi dengan mulai berlakunya Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang telah disahkan pada tanggal 17 Oktober 2022 sebagai wujud komitmen Negara dalam menjaga hak privasi dan keamanan informasi setiap individu. Dengan perkembangan teknologi yang pesat serta penetrasinya dalam pemilihan umum, maka membuka peluang bagi ancaman yang lebih luas dalam ranah siber. Intensitas, frekuensi dan tipe serangan yang pernah terjadi pada pemilu di beberapa negara, seharusnya dapat dipelajari oleh pihak KPU Provinsi Jambi untuk dapat mengidentifikasi pola serangan siber. Sehingga, ketika suatu serangan terjadi maka dapat diketahui tujuan (purpose), target (target), konteks (context), dan skala (scale). Serangan siber yang pernah dialami oleh KPU yang terus bereskalasi dalam frekuensi, dan publisitas dari tahun ke tahun menjadi tantangan tersendiri dalam membentuk keamanan siber. Dalam menghadapi spektrum ancaman siber yang luas dan dengan kemajuan teknologi pada saat ini, KPU Provinsi Jambi sepantasnya memiliki infrastruktur yang menunjang kinerjanya. Sehingga untuk menunjang kinerja tersebut, KPU Provinsi Jambi membangun kerjasama dengan instansi-instansi lainnya. Dalam pelaksanaan pemilu selama ini, KPU Provinsi Jambi telah bekerjasama dengan pihak Institusi-institusi seperti Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), Badan Intelijen Negara (BIN), Kementerian Koordinator Politik, Hukum dan Keamanan serta Cybercrime POLRI akan turut berkontribusi dalam melakukan deteksi, proteksi serta prevensi terhadap ancaman dan serangan siber yang dapat terjadi.

Di Indonesia, kejahatan siber meningkat seiring dengan kemajuan digital. Malware, phishing, DDoS (Distributed Denial of Service), cyberstalking, identitas palsu, cyberbullying, kejahatan finansial, dan serangan pada infrastruktur kritis adalah beberapa kejahatan cyber yang paling umum terjadi. Jumlah kebocoran data internet di Indonesia meningkat 143% dari kuartal pertama 2022 hingga kuartal kedua 2022, dengan 1,04 juta akun membocorkan data. Kasus kejahatan dunia maya telah berdampak pada orang dan lembaga pemerintah, berikut diantaranya:



Gambar 1 Kasus Kejahatan Keamanan Siber Di Indonesia
(Sumber : Antaranews.com)

METODE

Jenis penelitian yang digunakan dalam studi ini adalah Penelitian Tindakan (Action Research). Metode ini menitikberatkan pada langkah-langkah praktis yang bertujuan untuk mengatasi permasalahan yang tengah dihadapi. Dalam konteks penelitian ini, pendekatan Action Research dilakukan melalui wawancara dengan narasumber guna menyusun rancangan Sistem Manajemen Keamanan Informasi (SMKI) dengan mengacu pada kerangka kerja ISO/IEC 27001. Metode ini memungkinkan penulis untuk mengumpulkan data dari pengalaman dan perspektif para pemangku kepentingan seperti staf IT, manajer keamanan informasi, dan pengambil keputusan di KPU. Penulis juga terjun langsung ke lapangan untuk melakukan eksplorasi terhadap objek penelitian. Penulis juga menginterpretasi data yang telah dikumpulkannya.

HASIL DAN PEMBAHASAN

A. Hasil Observasi

Observasi ini dilakukan tanpa kontak langsung dengan objek yang diteliti. Artinya, data dikumpulkan tanpa terlibat secara aktif dalam kegiatan yang diamati. Teknik ini dikenal sebagai observasi pasif atau non-partisipatif. Langkah pertama adalah mengamati kondisi lingkungan, misalnya bagaimana perangkat seperti komputer disimpan dan dijaga, serta bagaimana informasi penting diakses dan diamankan. Langkah berikutnya adalah menelaah dokumen-dokumen yang ada, di mana peneliti mengumpulkan dan mempelajari berkas-berkas internal, seperti data keamanan, staf, dan sistem keamanan yang diterapkan.

B. Hasil Wawancara

Berdasarkan hasil wawancara dengan narasumber dari KPU Provinsi Jambi, diketahui bahwa lembaga ini memiliki peran utama dalam mengawasi, membimbing, dan memastikan kelancaran pelaksanaan pemilu di 13 KPU kabupaten/kota di wilayah Jambi. Tanggung jawab tersebut mencakup koordinasi dan pengawasan agar proses pemilu berjalan secara transparan dan akuntabel. Namun, dalam pelaksanaannya, KPU Provinsi Jambi menghadapi tantangan dalam hal keamanan sistem, terutama karena penggunaan satu jaringan untuk seluruh operasional yang menimbulkan risiko efisiensi dan kerentanan terhadap serangan siber.

Meski dengan keterbatasan sumber daya, mereka telah berupaya menjaga keamanan sistem dengan memanfaatkan alat pemantauan serangan secara real- time, walau belum mampu melakukan pemblokiran langsung terhadap ancaman. Meskipun hingga saat ini belum terjadi insiden besar yang mengganggu pelaksanaan pemilu, mereka pernah menerima notifikasi dari BSSN terkait potensi percobaan peretasan, serta mengalami gangguan teknis ringan. Untuk meningkatkan keamanan siber, KPU Provinsi Jambi bekerja sama dengan KPU RI dan berbagai instansi seperti Kominfo, BSSN, Polri, dan BIN untuk membentuk Cyber Security Response Team (CSRT). Dalam aspek regulasi, KPU Provinsi Jambi telah menerapkan Sistem Pemerintahan Berbasis Elektronik (SPBE) sesuai Peraturan Presiden Tahun 2018 dan Peraturan KPU Nomor 5 Tahun 2021 guna mendukung efisiensi dan akuntabilitas layanan. Namun, penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001 belum dilaksanakan secara resmi, meskipun mereka menyadari pentingnya standar ini dalam menjaga keamanan aset dan informasi penting. Saat ini, kebijakan internal mengenai keamanan informasi belum terdokumentasi secara sistematis dan masih bersifat prosedural. Oleh karena itu, pihak KPU menyambut baik usulan dari peneliti untuk membantu merancang kebijakan dan pedoman yang sesuai dengan ISO/IEC 27001.

Dalam tahap awal penerapan, KPU membutuhkan dokumen kebijakan yang mencakup ruang lingkup, peran, dan tanggung jawab terkait keamanan sistem informasi. Mereka juga

menekankan perlunya peningkatan kapasitas sumber daya manusia melalui pelatihan dan workshop karena sebagian besar pegawai masih membutuhkan pemahaman yang lebih dalam mengenai manajemen risiko informasi. Harapan jangka panjang KPU Provinsi Jambi terhadap penerapan standar ini adalah terwujudnya sistem informasi yang lebih kuat, terpercaya, dan transparan, serta tumbuhnya budaya kerja yang sadar akan pentingnya keamanan informasi dalam mendukung keberhasilan pemilu yang bersih dan demokratis

C. Perancangan Standar sesuai ISO 27001

Berdasarkan hasil wawancara, diketahui bahwa KPU Provinsi Jambi belum mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) yang berstandar ISO 27001. Hal ini bertujuan untuk mengurangi risiko terkait keamanan siber di lingkungan KPU. Menanggapi situasi tersebut, peneliti mengusulkan penyusunan dokumen kebijakan serta pedoman atau standar yang mengacu pada ISO 27001, yang disesuaikan dengan kebutuhan spesifik KPU Provinsi Jambi.

Dalam proses penyusunan dokumen ini, ruang lingkup dan batasan ditetapkan sesuai dengan konteks organisasi. Selanjutnya, kebijakan keamanan informasi dirumuskan, termasuk penetapan peran dan tanggung jawab yang jelas bagi pihak- pihak terkait. Berikut ini disajikan uraian mengenai langkah-langkah yang telah diambil dalam menyusun draft dokumen kebijakan dan pedoman standar ISO 27001. Untuk detail lengkap draft pedoman tersebut, dapat dilihat pada Lampiran.

D. Ruang Lingkup dan Batasan sesuai Konteks Organisasi

Dalam menyusun konteks organisasi ini dimana dalam pedoman ISO/IEC 27001 sesuai dengan klausal 4 yakni konteks organisasi, dimana mengacu pada lingkungan operasional dari KPU Provinsi Jambi. Bagian diperlukan untuk mengidentifikasi faktor eksternal dan internalnya.

1. Faktor Internal dan Eksternal

Dalam penyusunan dan analisis dari kasus eksternal KPU Provinsi Jambi dapat mengacu pada PESTLE (Politik, Ekonomi, Sosial, Teknologi, Lingkungan, dan Legal) yang menjadi alat bantu untuk mengidentifikasi tantangan eksternal yang dihadapi KPU. Semua aspek yang mengarah pada keamanan informasi akan dianalisis berdasarkan kategori isu politik, ekonomi, sosial, teknologi, lingkungan serta legal. Pada analisis faktor internal yang cukup berbeda dari faktor eksternal, KPU Provinsi Jambi yang berfokus pada beberapa layanan, pengelolaan data, ketersediaan sumber daya dan infrastruktur teknologi.

Dengan ini KPU Provinsi Jambi dapat memahami bahwa ancaman seperti serangan terhadap sistem informasi pemilu (SPBE) dapat mempengaruhi kredibilitas proses demokrasi serta menilai sejauh mana infrastruktur dan kebijakan ini mendukung keamanan informasi.

2. Stakeholders

Manajemen keamanan informasi melibatkan berbagai pihak, termasuk pegawai, divisi IT, dan manajemen KPU Provinsi Jambi. Selain itu, pemerintah, lembaga penegak hukum, serta masyarakat umum juga menjadi bagian dari pemangku kepentingan yang memiliki peran dan harapan terhadap transparansi dan integritas data pemilu.

3. Ruang Lingkup

Cakupan Sistem Manajemen Keamanan Informasi (SMKI) meliputi seluruh sistem SPBE, termasuk data pemilih, aplikasi pendukung pemilu, dan jaringan internal KPU. Ruang lingkup ini juga mencakup KPU Kabupaten/Kota untuk memastikan standar keamanan informasi yang seragam.

Penetapan ruang lingkup ini mempertimbangkan kebutuhan KPU Provinsi Jambi dalam mengelola keamanan informasi, dengan fokus pada menjaga kerahasiaan

(confidentiality), integritas (integrity), dan ketersediaan (availability) data serta informasi yang digunakan dalam sistem dan aplikasi pemilu.

E. Kebijakan

Untuk menjaga kerahasiaan data pemilih dan sistem pemilu dari ancaman siber, dan memberikan keyakinan kepada masyarakan bahwa sistem KPU aman dan transparan, serta memastikan bahwa KPU Provinsi Jambi mematuhi aturan keamanan informasi yang relevan di tingkat nasional dan internasional. Dimana hal ini perlu tersertifikasi dengan SNI ISO 27001. Sehingga untuk mencegah keamanan siber, KPU Provinsi Jambi dapat menerapakan kebijakan berbasis ISO/IEC 27001 yang mencakup :

1. Kebijakan keamanan informasi, mengatur perlindungan data pemilih, sistem SPBE, dan operasional KPU.
2. Manajemen Risiko. Mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan, seperti peretasan dan kebocoran data, dengan mitigasi seperti firewall dan enkripsi.
3. Pengelolaan aset informasi, dimana melindungi aset penting, termasuk data pemilih, sistem SPBE, dengan kontrol akses dan pencadangan data.
4. Pengendalian akses, dengan membatasi askes hanya untuk pihak yang berwenang dengan autentikasi ganda dan monitoring aktivitas pengguna.
5. Penanganan insiden siber, dengan menyusun prosedur deteksi, pelaporan, respons, dan evaluasi insiden keamanan, bekerja sama dengan CSIRT.
6. Kesadaran dan Pelatihan, KPU Provinsi dapat meningkatkan pemahaman staf KPU tentang ancaman siber melalui pelatihan dan edukasi.
7. Audit dan Pemantauan, KPU harus melakukan audit dan monitoring berkala untuk memastikan kebijakan diterapkan dengan baik dan ancaman terdeteksi dini.

F. Peran dan Tanggung Jawab

Pembagian tugas dan kewenangan yang diterapkan dalam penerapan kebijakan keamanan informasi berbasis ISO/IEC 27001 di KPU Provinsi Jambi dalam memastikan bahwa sistem keamanan informasi berjalan dengan optimal sehingga mampu mencegah ancaman keamanan siber yakni sebagai berikut :

1. Pimpinan – Kepala KPU Provinsi Jambi
   a. Sebagai pemimpin di tingkat Provinsi yang bertanggung jawab atas implementasi sistem keamanan informasi.
   b. Menyetujui kebijakan keamanan informasi berbasis ISO/IEC 27001.
   c. Memastikan sumber daya yang memadai untuk penerapan kebijakan.
   d. Mengawasi efektivitas penerapan kebijakan keamanan informasi.
2. Tim Manajemen Keamanan Informasi (Tim SMKI)
   a. Tim khusus yang bertanggung jawab atas perancangan, penerapan, pemantauan, dan perbaikan sistem keamanan informasi.
   b. Mengidentifikasi risiko keamanan informasi dan menentukan langkah mitigasi.
   c. Mengawasi kepatuhan terhadap standar ISO/IEC 27001.
   d. Melakukan audit keamanan informasi secara berkala.
   e. Menyusun prosedur untuk menangani insiden keamanan siber.
3. Divisi IT KPU Provinsi Jambi
   a. Menjadi pelaksana teknis untuk memastikan perlindungan aset digital dan operasional SPBE.
   b. Mengelola infrastruktur IT seperti jaringan, server, dan aplikasi SPBE.
   c. Menerapkan kontrol teknis seperti firewall, enkripsi, dan sistem monitoring.
   d. Melakukan backup data secara rutin dan mengamankan akses sistem.
   e. Berkolaborasi dengan tim CSIRT untuk menangani insiden siber.

4. Pegawai KPU dan Operator SPBE
   a. a. Sebagai pengguna utama sistem yang bertanggung jawab untuk mematuhi kebijakan keamanan informasi.
   b. Mengikuti pelatihan keamanan informasi.
   c. Menggunakan sistem informasi sesuai prosedur yang ditetapkan.
   d. Melaporkan potensi ancaman atau insiden keamanan kepada tim IT.
   e. Menjaga kerahasiaan informasi yang diakses.
5. Badan Pengawas Pemilu (Bawaslu)
   a. Sebagai pengawas untuk memastikan bahwa KPU mematuhi regulasi dan standar keamanan informasi.
   b. Mengawasi implementasi kebijakan keamanan informasi di KPU.
   c. Melakukan audit independen terkait keamanan informasi.
   d. Memberikan rekomendasi untuk peningkatan keamanan berdasarkan temuan.
6. Mitra Eksternal (Kominfo, BSSN, Polri, BIN, Telkom)
   a. Sebagai lembaga pendukung yang memberikan panduan, bantuan teknis, dan perlindungan tambahan.
   b. Memberikan pelatihan teknis terkait keamanan informasi kepada KPU.
   c. Membantu KPU dalam mengembangkan kebijakan berbasis ISO/IEC 27001.
   d. Mendukung penanganan insiden siber besar melalui koordinasi lintas lembaga.
7. Masyarakat
   a. Sebagai penerima manfaat dari sistem keamanan informasi dan pengawas tidak langsung.
   b. Menyampaikan laporan atau keluhan jika ada indikasi pelanggaran keamanan informasi dan memberikan dukungan moral terhadap upaya KPU untuk meningkatkan keamanan sistem.

G. Tahap Check

Pada tahap Check, dilakukan peninjauan internal terhadap draft awal dokumen kebijakan keamanan informasi berbasis ISO/IEC 27001 yang telah dirancang. Proses evaluasi ini dilaksanakan melalui diskusi terstruktur bersama dua pihak utama di lingkungan KPU Provinsi Jambi, yaitu Kepala Subbagian Perencanaan Data dan Informasi serta Komisioner Divisi Perencanaan Data dan Informasi. Diskusi ini bertujuan untuk menilai sejauh mana isi dokumen tersebut sesuai dengan kebutuhan operasional di lapangan dan untuk memastikan bahwa kebijakan yang disusun mampu mengantisipasi berbagai potensi risiko keamanan informasi. Berdasakan hasil diskusi, diperoleh beberapa temuan penting, yakni :

1. Kontrol akses yang perlu diperjelas, terdapat kebutuhan untuk memperkuat prosedur pengelolaan hak akses pengguna, termasuk dalam hal autentikasi, otorisasi, serta pencabutan hak akses bila pegawai pindah divisi atau berhenti.
2. Perlunya program pelatihan kesadaran keamanan informasi, Banyak pegawai masih belum memahami pentingnya menjaga kerahasiaan informasi, terutama dalam penggunaan email, password, serta pengelolaan data elektronik.
3. Pentingnya audit dan review berkala, disarankan untuk menyusun prosedur audit internal agar setiap tahun dapat dilakukan penilaian terhadap efektivitas pengelolaan keamanan informasi.
4. Sistem manajemen insiden harus lebih rinci, harus ada prosedur standar tentang bagaimana menangani kejadian keamanan, mulai dari pelaporan insiden hingga analisis penyebab dan langkah perbaikannya.

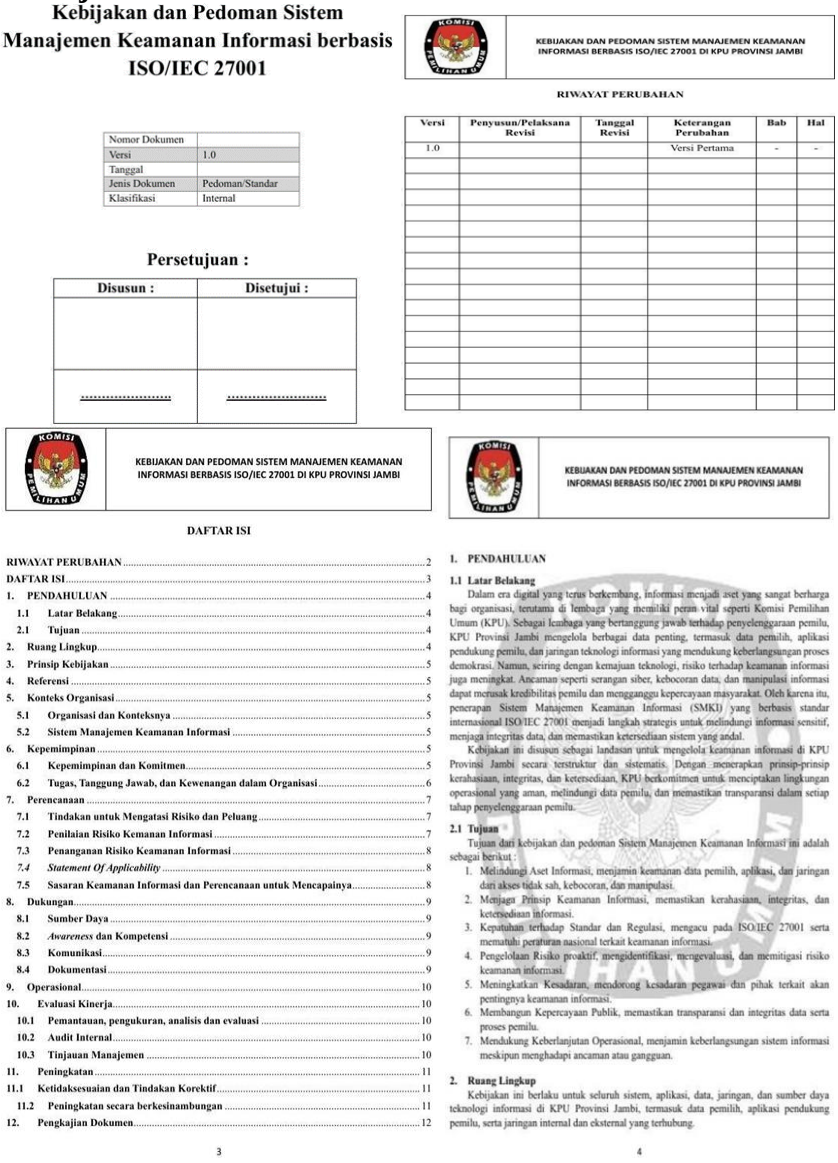
Melalui hasil evaluasi ini, terlihat bahwa draft dokumen telah mengarah ke jalur yang

benar, namun masih memerlukan beberapa penyempurnaan agar lebih komprehensif dan operasional.

H. Tahap Act

Tahap Act menjadi puncak dari siklus PDCA, di mana tindakan nyata diambil untuk memperbaiki dan memperkuat sistem berdasarkan hasil evaluasi sebelumnya. Revisi dokumen, penyusunan rencana pelatihan, penerapan audit internal, serta perencanaan peningkatan infrastruktur TI menunjukkan upaya serius untuk mengimplementasikan SMKI secara berkelanjutan. Strategi continuous improvement (peningkatan berkelanjutan) yang diadopsi dalam kebijakan juga menunjukkan bahwa KPU Provinsi Jambi tidak hanya ingin memenuhi standar, tetapi juga berkomitmen untuk terus menyesuaikan sistem terhadap perubahan ancaman keamanan informasi. Langkah-langkah ini sesuai dengan prinsip dasar ISO/IEC 27001 yang menekankan pentingnya tinjauan berkala, tindakan korektif, dan adaptasi terhadap dinamika baru. Berikut adalah hasil dari dokumen kebijakan dan pedoman SMKI berbasis ISO/IEC 27001 yang telah melalu tahap evaluasi dan perbaikan.

I. Dokumen Kebijakan dan Pedoman SMKI berbasis ISO/IEC 27001



Kebijakan dan Pedoman Sistem Manajemen Keamanan Informasi berbasis ISO/IEC 27001

Nomor Dokumen	
Versi	1.0
Tanggal	
Jenis Dokumen	Pedoman/Standar
Klasifikasi	Internal

Persetujuan :

Disusun :	Disetujui :
.....	.....

KEBIJAKAN DAN PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001 DI KPU PROVINSI JAMBI

RIWAYAT PERUBAHAN

Versi	Penyusun/Pelaksana Revisi	Tanggal Revisi	Keterangan Perubahan	Bab	Hal
1.0			Versi Pertama	-	-

KEBIJAKAN DAN PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001 DI KPU PROVINSI JAMBI

DAFTAR ISI

3

KEBIJAKAN DAN PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001 DI KPU PROVINSI JAMBI

1. PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang terus berkembang, informasi menjadi aset yang sangat berharga bagi organisasi, terutama di lembaga yang memiliki peran vital seperti Komisi Pemilihan Umum (KPU). Sebagai lembaga yang bertanggung jawab terhadap penyelenggaraan pemilu, KPU Provinsi Jambi mengelola berbagai data penting, termasuk data pemilih, aplikasi pendukung pemilu, dan jaringan teknologi informasi yang mendukung keberlangsungan proses demokrasi. Namun, seiring dengan kemajuan teknologi, risiko terhadap keamanan informasi juga meningkat. Ancaman seperti serangan siber, kebocoran data, dan manipulasi informasi dapat merusak kredibilitas pemilu dan mengganggu kepercayaan masyarakat. Oleh karena itu, penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang berbasis standar internasional ISO/IEC 27001 menjadi langkah strategis untuk melindungi informasi sensitif, menjaga integritas data, dan memastikan ketersediaan sistem yang andal.

Kebijakan ini disusun sebagai landasan untuk mengelola keamanan informasi di KPU Provinsi Jambi secara terstruktur dan sistematis. Dengan menerapkan prinsip-prinsip kerahasiaan, integritas, dan ketersediaan, KPU berkomitmen untuk menciptakan lingkungan operasional yang aman, melindungi data pemilu, dan memastikan transparansi dalam setiap tahap penyelenggaraan pemilu.

2.1 Tujuan

Tujuan dari kebijakan dan pedoman Sistem Manajemen Keamanan Informasi ini adalah sebagai berikut :

1. Melindungi Aset Informasi, menjamin keamanan data pemilih, aplikasi, dan jaringan dari akses tidak sah, kebocoran, dan manipulasi.
2. Menjaga Prinsip Keamanan Informasi, memastikan kerahasiaan, integritas, dan ketersediaan informasi.
3. Kepatuhan terhadap Standar dan Regulasi, mengacu pada ISO/IEC 27001 serta mematuhi peraturan nasional terkait keamanan informasi.
4. Pengelolaan Risiko proaktif, mengidentifikasi, mengevaluasi, dan memitigasi risiko keamanan informasi.
5. Meningkatkan Kesadaran, mendorong kesadaran pegawai dan pihak terkait akan pentingnya keamanan informasi.
6. Membangun Kepercayaan Publik, memastikan transparansi dan integritas data serta proses pemilu.
7. Mendukung Keberlanjutan Operasional, menjamin keberlangsungan sistem informasi meskipun menghadapi ancaman atau gangguan.

2. Ruang Lingkup

Kebijakan ini berlaku untuk seluruh sistem, aplikasi, data, jaringan, dan sumber daya teknologi informasi di KPU Provinsi Jambi, termasuk data pemilih, aplikasi pendukung pemilu, serta jaringan internal dan eksternal yang terhubung.

4

3. Prinsip Kebijakan

- Kerahasiaan (Confidentiality) yaitu melindungi informasi dari akses yang tidak sah.
- Integritas (Integrity) yaitu memastikan informasi tetap akurat dan tidak dimodifikasi tanpa izin.
- Ketersediaan (Availability) yakni menjamin informasi dapat diakses saat diperlukan.

4. Referensi

- Persyaratan SMKI SNI ISO/IEC 27001
- Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik.

5. Konteks Organisasi

5.1 Organisasi dan Konteksnya

Konteks organisasi dalam Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001 di KPU Provinsi Jambi mencakup pemahaman terhadap faktor internal dan eksternal yang mempengaruhi keberhasilan implementasi keamanan informasi. Faktor eksternal dianalisis menggunakan metode PESTLE (politik, ekonomi, sosial, teknologi, lingkungan, dan legal), sedangkan faktor internal meliputi proses operasional, sumber daya manusia, dan infrastruktur teknologi. Selain itu, kebutuhan dan harapan pihak terkait, seperti pegawai, divisi IT, manajemen KPU, pemerintah, dan masyarakat umum, menjadi pertimbangan utama dalam perancangan kebijakan.

5.2 Sistem Manajemen Keamanan Informasi

Cakupan Sistem Manajemen Keamanan Informasi (SMKI) meliputi seluruh sistem SPBE, infrastruktur teknologi, serta unit operasional yang relevan, dengan penekanan pada menjaga kerahasiaan, integritas, dan ketersediaan informasi. Oleh karena itu, SMKI dirancang untuk mengamankan data pemilu, memastikan kepatuhan terhadap regulasi, meningkatkan kepercayaan masyarakat, dan mendukung operasional yang andal serta aman.

6. Kepemimpinan

6.1 Kepemimpinan dan Komitmen

Untuk melindungi kerahasiaan data pemilih dan sistem pemilu dari ancaman siber, serta memberikan keyakinan kepada masyarakat bahwa sistem KPU aman, transparan, dan sesuai dengan regulasi keamanan informasi nasional maupun internasional, KPU Provinsi Jambi perlu menerapkan keamanan berbasis ISO/IEC 27001 yang tersertifikasi SNI ISO 27001. Langkah tersebut mencakup:

a. Kebijakan Keamanan Informasi: Mengatur perlindungan data pemilih, sistem SPBE, dan operasional KPU.
b. Manajemen Risiko: Mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan seperti peretasan dan kebocoran data melalui mitigasi, termasuk firewall dan enkripsi.
c. Pengelolaan Aset Informasi: Melindungi aset penting seperti data pemilih dan sistem SPBE dengan kontrol akses dan pencadangan data.

- Memberikan rekomendasi untuk peningkatan keamanan berdasarkan temuan.

f. Mitra Eksternal (Kominfo, BSSN, Polri, BIN)
- Sebagai lembaga pendukung yang memberikan panduan, bantuan teknis, dan perlindungan tambahan.
- Memberikan pelatihan teknis terkait keamanan informasi kepada KPU.
- Membantu KPU dalam mengembangkan kebijakan berbasis ISO/IEC 27001.
- Mendukung penanganan insiden siber besar melalui koordinasi lintas lembaga.

g. Masyarakat
- Sebagai penerima manfaat dari sistem keamanan informasi dan pengawas tidak langsung.
- Menyampaikan laporan atau keluhan jika ada indikasi pelanggaran keamanan informasi dan memberikan dukungan moral terhadap upaya KPU untuk meningkatkan keamanan sistem.

7. Perencanaan

7.1 Tindakan untuk Mengatasi Risiko dan Peluang

Perencanaan harus mencakup identifikasi risiko dan peluang yang dapat mempengaruhi keamanan informasi dan keberhasilan SMKI, prosesnya mencakup identifikasi ancaman dan kerentanan yang relevan, analisis dampak dan kemungkinan terjadinya risiko dan perencanaan tindakan mitigasi untuk meminimalkan dampak risiko. Tindakan ini bertujuan untuk:

- Mengatasi risiko yang dapat mengancam keamanan informasi, seperti serangan siber, kebocoran data, atau kerusakan sistem.
- Memanfaatkan peluang untuk memperkuat keamanan informasi, misalnya melalui inovasi teknologi atau pengembangan kebijakan baru.

Proses manajemen risiko keamanan informasi diterapkan dengan menghasilkan *output* berupa :

- Profil risiko keamanan informasi yang mencakup aset penting terkait kemanan informasi dari KPU Provinsi Jambi.
- Rencana peningkatan tindakan pengendalian risiko *(Risk Treatment Plan)* keamanan informasi di KPU Provinsi Jambi.

Proses pelaksanaan manajemen risiko harus dilakukan setidaknya sekali dalam satu tahun, dan hasil atau *output* dari proses manajemen risiko ini harus mendapatkan persetujuan terlebih dahulu sebelum diterapkan.

7.2 Penilaian Risiko Kemanan Informasi

Untuk memastikan kontrol keamanan informasi berjalan secara efektif, KPU Provinsi Jambi perlu melaksanakan evaluasi risiko keamanan yang berkaitan dengan sistem di lingkup KPU Provinsi Jambi. Proses ini melibatkan pendefinisian langkah-langkah dalam penerapan penilaian risiko keamanan informasi yang mencakup :

a. Melakukan identifikasi risiko keamanan informasi yang mencakup pelaksanaan proses penilaian risiko secara menyeluruh,
b. Menganalisis setiap risiko keamanan informasi, mencakup :
- Menilai dampak potensial yang mungkin terjadi,
- Mengevaluasi kemungkinan terjadinya risiko yang telah diidentifikasi,
- Menentukan tingkat risiko berdasarkan hasil analisis,

- Menetapkan pemilik risiko *(risk owner)* untuk masing-masing risiko yang teridentifikasi.

c. Melakukan evaluasi terhadap setiap risiko keamanan informasi, meliputi:
- Membandingkan hasil analisis risiko dengan kriteria risiko yang telah ditetapkan,
- Memberikan prioritas terhadap risiko yang telah dianalisis untuk menentukan langkah penanganannya.

Proses penilaian risiko dilakukan secara rutin atau saat terdapat usulan maupun perubahan signifikan pada Sistem Manajemen Keamanan Informasi yang mengacu pada standar ISO/IEC 27001. Penilaian ini juga mempertimbangkan kriteria risiko keamanan informasi yang telah ditetapkan. Detail mengenai proses tersebut dijelaskan dalam Metodologi *Risk Assessment*.

7.3 Penanganan Risiko Keamanan Informasi

Penanggung Jawab Risiko *(risk owner)* di KPU Provinsi Jambi bertanggung jawab untuk menentukan langkah penanganan risiko keamanan informasi dengan cara:

- Memilih opsi penanganan risiko yang sesuai berdasarkan hasil penilaian risiko,
- Menentukan kontrol yang diperlukan untuk mengimplementasikan opsi penanganan risiko keamanan yang dipilih,
- Menyusun rencana penanganan risiko keamanan informasi yang dituangkan dalam dokumen rencana penanganan risiko.

7.4 Statement Of Applicability

Bagian ini mencakup kontrol pengendalian keamanan informasi yang relevan untuk KPU Provinsi Jambi, termasuk kontrol yang sudah diterapkan sebelumnya. Pemilihan kontrol tersebut dilakukan selama aktivitas penanganan risiko sebagai bagian dari proses manajemen risiko, dengan mempertimbangkan kontrol keamanan informasi yang direkomendasikan oleh standar SNI 27001. Penjelasan mengenai penerapan kontrol keamanan informasi sesuai dengan SNI 27001 dapat ditemukan dalam dokumen *statement of applicability*.

7.5 Sasaran Keamanan Informasi dan Perencanaan untuk Mencapainya

Tujuan keamanan informasi ditetapkan oleh manajemen puncak KPU Provinsi Jambi berdasarkan hasil evaluasi risiko yang telah dilakukan. Tujuan ini menjadi pedoman dalam mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada standar ISO/IEC 27001, sesuai dengan kontrol keamanan informasi yang berlaku. Evaluasi tujuan tersebut harus dilakukan setiap tahun dengan mempertimbangkan profil risiko yang teridentifikasi.

Penetapan tujuan keamanan informasi harus mencakup :

- Identifikasi sasaran yang perlu dicapai,
- Sumber daya yang diperlukan,
- Penanggung jawab pelaksanaan tujuan,
- Batas waktu penyelesaian,
- Dan mekanisme untuk mengevaluasi pencapaian tujuan tersebut.

Berikut ini adalah tabel yang merangkum sasaran keamanan informasi dan rincian elemen yang mendukung pencapaian tujuan tersebut :

Aspek	Keterangan
Tujuan	Sasaran yang ingin dicapai terkait keamanan informasi, seperti melindungi kerahasiaan, integritas, dan ketersediaan data.
Sumber Daya	Sumber daya yang diperlukan, seperti perangkat lunak, perangkat keras, tenaga ahli, atau anggaran.
Penanggung Jawab	Individu atau tim yang bertanggung jawab untuk memastikan pelaksanaan sasaran keamanan informasi.
Target Penyelesaian	Waktu atau tenggat yang ditetapkan untuk mencapai tujuan keamanan informasi.
Evaluasi Hasil	Metode atau mekanisme yang digunakan untuk menilai keberhasilan dan efektivitas sasaran, seperti audit atau penilaian ulang.

8. Dukungan

8.1 Sumber Daya

Kepala KPU bersama dengan Tim Manajemen SMKI bertanggung jawab untuk menetapkan dan menyediakan sumber daya yang diperlukan dalam pembentukan, pelaksanaan, pemeliharaan, dan peningkatan berkelanjutan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001. Sumber daya ini mencakup tenaga kerja, serta sarana dan prasarana lain yang dibutuhkan untuk memastikan implementasi ISO/IEC 27001 berjalan efektif. Tujuannya adalah melindungi KPU Provinsi Jambi dari ancaman siber sekaligus menjaga tingkat keandalan sistem sesuai dengan standar yang diharapkan.

8.2 *Awareness* dan Kompetensi

Kesadaran terkait keamanan informasi di KPU Provinsi Jambi harus dipahami dan diterapkan oleh seluruh pegawai serta pihak terkait. Hal ini bertujuan agar setiap individu memahami kontrol keamanan informasi yang perlu diterapkan dalam lingkungan kerja KPU Provinsi Jambi.

Pimpinan KPU Provinsi Jambi bertanggung jawab untuk memastikan bahwa seluruh pegawai memiliki kompetensi yang sesuai dengan persyaratan yang telah ditetapkan dalam uraian jabatan masing-masing. Selain itu, pimpinan juga wajib menyediakan pelatihan yang diperlukan untuk meningkatkan kemampuan pegawai dalam mendukung pelaksanaan tugas mereka.

8.3 Komunikasi

Komunikasi antar fungsi dalam menjalankan kontrol keamanan informasi di KPU Provinsi Jambi menjadi bagian penting dari Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada standar ISO/IEC 27001. Tujuan dari komunikasi ini adalah untuk memperlancar koordinasi antar fungsi serta meningkatkan efektivitas penerapan SMKI berbasis ISO/IEC 27001.

8.4 Dokumentasi

Dalam penerapan ISO/IEC 27001, diperlukan serangkaian dokumen yang berisi aturan untuk memastikan bahwa seluruh proses dijalankan secara konsisten. Sistem Manajemen Keamanan Informasi dijelaskan dalam dokumen yang disusun dengan struktur berikut:

- Pedoman Sistem Manajemen Keamanan Informasi ISO/IEC 27001 yang berisi gambaran umum tentang sistem manajemen keamanan informasi, kebijakan keamanan informasi, serta kesesuaiannya dengan standar nasional SNI 27001.
- Prosedur yang menjelaskan secara rinci metode dan langkah-langkah dalam menjalankan sistem manajemen keamanan informasi sesuai dengan ISO/IEC 27001.
- Dokumen Pendukung yang memiliki fungsi sebagai penunjang prosedur dan instruksi kerja, seperti formulir, catatan hasil kegiatan, serta dokumen lain yang mendukung pelaksanaan sistem.

Penerapan dan pengendalian kebijakan serta pedoman sistem manajemen keamanan informasi berbasis ISO/IEC 27001 harus mencakup proses identifikasi, penyimpanan, perlindungan, pengambilan kembali, penentuan masa penyimpanan (retensi), serta pengelolaan dokumentasi.

9. Operasional

Dalam menjalankan ISO/IEC 27001, pimpinan KPU Provinsi Jambi perlu menyusun program rencana penanganan risiko sebagai bagian dari implementasi sistem ini. Program tersebut harus mencakup langkah-langkah yang harus dilakukan, siapa yang bertanggung jawab atas setiap tugas, serta target penyelesaiannya. Setiap langkah dalam program ini harus dipantau dan dievaluasi secara berkala untuk memastikan bahwa tujuan yang telah ditetapkan dapat tercapai dengan baik.

10. Evaluasi Kinerja

10.1 Pemantauan, pengukuran, analisis dan evaluasi

Pimpinan KPU Provinsi Jambi bertanggung jawab untuk mengevaluasi sejauh mana kontrol keamanan informasi telah diterapkan serta menilai efektivitas Sistem Manajemen Keamanan Informasi (SMKI) yang berpedoman pada standar ISO/IEC 27001.

Proses evaluasi ini dilakukan melalui pemantauan, pengukuran, analisis, dan penunjauan terhadap sistem yang berjalan. Seluruh langkah tersebut mengacu pada metode yang digunakan untuk menilai efektivitas penerapan ISO/IEC 27001. Selain itu, setiap hasil pemantauan dan pengukuran harus didokumentasikan dengan baik sebagai bukti bahwa proses evaluasi telah dilakukan. Dokumentasi ini juga berfungsi sebagai dasar untuk perbaikan dan peningkatan berkelanjutan dalam penerapan keamanan informasi di lingkungan KPU Provinsi Jambi.

10.2 Audit Internal

KPU Provinsi Jambi memiliki kewenangan untuk menentukan pelaksanaan audit internal sesuai dengan kebutuhan organisasi. Sebagai panduan, audit internal wajib dilaksanakan setidaknya satu kali dalam setahun. Audit ini mencakup seluruh aspek penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO/IEC 27001, sebagaimana diatur dalam dokumen yang telah ditetapkan. Tujuan utama dari audit internal ini adalah untuk mengidentifikasi peluang perbaikan dalam sistem, serta mendeteksi dan mengatasi ketidaksesuaian yang terjadi, termasuk mengeliminasi akar penyebabnya secepat mungkin. Hal ini bertujuan untuk menjaga agar sistem tetap berjalan sesuai dengan standar yang ditetapkan dan terus ditingkatkan

10.3 Tinjauan Manajemen

Pimpinan KPU Provinsi Jambi secara rutin melakukan tinjauan terhadap penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada standar ISO/IEC 27001.

Tinjauan ini dilakukan dalam interval waktu satu tahun sekali. Tujuan dari tinjauan ini adalah untuk mengevaluasi sejauh mana sistem keamanan informasi telah diimplementasikan sesuai dengan standar yang berlaku. Proses tinjauan mencakup penilaian terhadap efektivitas pelaksanaan kontrol keamanan informasi, identifikasi kekurangan atau ketidaksesuaian yang perlu diperbaiki, serta pengukuran terhadap pencapaian tujuan keamanan informasi yang telah ditetapkan.

Hasil tinjauan ini kemudian dijadikan dasar untuk merumuskan langkah-langkah perbaikan dan peningkatan berkelanjutan pada implementasi SMKI berbasis ISO/IEC 27001. Dengan cara ini, KPU Provinsi Jambi dapat memastikan bahwa sistem keamanan informasi yang diterapkan tidak hanya sesuai standar, tetapi juga mampu menghadapi tantangan baru dalam menjaga keamanan data dan informasi.

11. Peningkatan

11.1 Ketidaksesuaian dan Tindakan Korektif

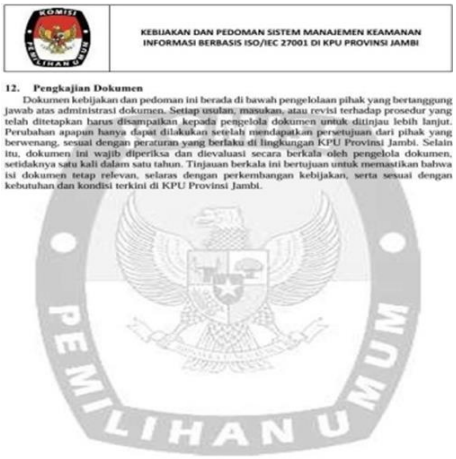
Pegawai atau pihak yang berwenang di KPU Provinsi Jambi bertanggung jawab untuk menindaklanjuti setiap ketidaksesuaian yang terjadi serta menghilangkan akar penyebabnya. Langkah-langkah yang dilakukan meliputi:

- Menangani ketidaksesuaian yang muncul.
- Mengevaluasi kebutuhan untuk mengatasi akar penyebab ketidaksesuaian guna mencegah terulangnya kejadian serupa atau munculnya permasalahan di tempat lain, dengan meninjau serta mengidentifikasi penyebab utama ketidaksesuaian.
- Melaksanakan tindakan yang diperlukan untuk mengoreksi ketidaksesuaian.
- Mengevaluasi efektivitas tindakan korektif yang telah diterapkan.
- Memastikan bahwa tindakan korektif yang diambil sesuai dengan tingkat dampak ketidaksesuaian yang terjadi.
- Mencatat dan mendokumentasikan ketidaksesuaian beserta tindakan korektif yang telah dilakukan sebagai bukti penanganan dan tindak lanjut, termasuk hasil dari tindakan yang diterapkan.

11.2 Peningkatan secara berkesinambungan

Untuk memastikan sistem manajemen keamanan informasi (SMKI) berbasis ISO/IEC 27001 berjalan secara optimal, pimpinan KPU Provinsi Jambi harus terus melakukan upaya peningkatan efektivitas secara berkelanjutan. Peningkatan ini dilakukan dengan menetapkan serta mengimplementasikan kebijakan SMKI yang jelas dan terarah, menentukan sasaran keamanan informasi yang sesuai dengan kebutuhan organisasi, serta mengacu pada hasil audit internal maupun eksternal sebagai bahan evaluasi. Selain itu, pimpinan juga perlu melakukan analisis menyeluruh terhadap setiap insiden keamanan informasi yang terjadi guna memahami penyebab serta dampaknya, sehingga dapat merumuskan langkah-langkah perbaikan yang tepat. Langkah-langkah ini mencakup tindakan korektif untuk mengatasi kelemahan yang ada serta tindakan pencegahan agar insiden serupa tidak terjadi di masa mendatang.

Seluruh proses peningkatan efektivitas SMKI ini harus didukung dengan tinjauan manajemen yang komprehensif, di mana pimpinan secara berkala mengevaluasi implementasi kebijakan, efektivitas langkah-langkah yang telah diambil, serta mengidentifikasi peluang perbaikan lebih lanjut demi memastikan bahwa sistem keamanan informasi di lingkungan KPU Provinsi Jambi tetap terjaga, andal, dan sesuai dengan standar ISO/IEC 27001.


KEBIJAKAN DAN PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO/IEC 27001 DI KPU PROVINSI JAMBI

12. Pengkajian Dokumen

Dokumen kebijakan dan pedoman ini berada di bawah pengelolaan pihak yang bertanggung jawab atas administrasi dokumen. Setiap usulan, masukan, atau revisi terhadap prosedur yang telah ditetapkan harus disampaikan kepada pengelola dokumen untuk ditinjau lebih lanjut. Perubahan apapun hanya dapat dilakukan setelah mendapatkan persetujuan dari pihak yang berwenang, sesuai dengan peraturan yang berlaku di lingkungan KPU Provinsi Jambi. Selain itu, dokumen ini wajib diperiksa dan dievaluasi secara berkala oleh pengelola dokumen, setidaknya satu kali dalam satu tahun. Tinjauan berkala ini bertujuan untuk memastikan bahwa isi dokumen tetap relevan, selaras dengan perkembangan kebijakan, serta sesuai dengan kebutuhan dan kondisi terkini di KPU Provinsi Jambi.

12

KESIMPULAN

Penelitian ini mengungkap bahwa sistem keamanan informasi (cybersecurity) di KPU Provinsi Jambi masih perlu diperkuat agar dapat sepenuhnya memenuhi standar ISO/IEC 27001. Walaupun telah dilakukan berbagai upaya awal, seperti penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan penggunaan alat pemantauan serangan siber, langkah-langkah tersebut belum sepenuhnya memenuhi ketentuan yang ditetapkan dalam standar ISO/IEC 27001.

Sebagai hasil dari penelitian ini, telah disusun rancangan awal berupa dokumen kebijakan dan pedoman penerapan standar ISO 27001. KPU Provinsi Jambi disarankan untuk segera mengimplementasikan standar ini secara menyeluruh, termasuk dalam penyusunan dokumen manajemen risiko, seperti risk register, analisis risiko, serta strategi mitigasi yang terstruktur guna meningkatkan perlindungan terhadap informasi sensitif.

Penerapan ISO 27001 memberikan kerangka kerja yang sistematis bagi KPU Provinsi Jambi dalam mengelola berbagai risiko yang berkaitan dengan keamanan informasi. Proses ini mencakup identifikasi dan penilaian risiko, penerapan langkah-langkah pengendalian keamanan, serta pemantauan dan evaluasi kinerja sistem keamanan. Dengan menerapkan standar ini, KPU Provinsi Jambi dapat lebih efektif dalam mengidentifikasi, menganalisis, dan menangani ancaman yang berpotensi mengganggu kerahasiaan, integritas, serta ketersediaan informasi. Oleh karena itu, ISO 27001 berperan penting dalam memperkuat sistem manajemen risiko, khususnya dalam ranah teknologi informasi.

DAFTAR PUSTAKA

Anggraeni, E. Y. (2019). Pengantar sistem informasi. Penerbit Andi.

Al Faruq, B., Herlianto, H. R., Simbolon, S. H., Utama, D. N., & Wibowo, A. (2020). Integration of ITIL V3, ISO 20000 & iso 27001: 2013forit services and security management system. International Journal, 9(3).

Arifin Z (2021) 'MSIM4404 – Keamanan Jaringan', pp. 1–37.

Ardyan, E., Boari, Y., Akhmad, A., Yuliyani, L., Hildawati, H., Suarni, A., ... & Judijanto, L. (2023). Metode Penelitian Kualitatif dan Kuantitatif: Pendekatan Metode Kualitatif dan Kuantitatif di Berbagai Bidang. PT. Sonpedia Publishing Indonesia.

Budi, E., Wira, D. and Infantono, A. (2021) 'Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0', Prosiding Seminar Nasional Sains Teknologi dan

Inovasi Indonesia (SENASTINDO), 3(November), pp. 223–234.
Calder, A., & Watkins, S. (2019). Information security risk management for ISO 27001/ISO 27002. It Governance Ltd.
Chantica, J. A., Cahyani, R., & Romadhon, A. (2022). Peranan Manajemen Pengawasan: Komitmen, Perencanaan, Kemampuan Karyawan (Literature Review Msdm). Jurnal Ilmu Manajemen Terapan, 3(3), 247-256.
Hakim, L.N. (2023) 'Standar Manajemen Keamanan Informasi (Smki) 27001:2022 DalamPenyelenggaraan Sistem Pemerintahan Berbasis ElektronikDi Pemerintah Daerah'.
Hartati, T., Mindara, G.P. and Mindara, C.L. (2023) 'Sistem Manajemen Keamanan Informasi Perlindungan Nilai Matakuliah berbasis ISO 27001', Jurnal ICT : Information Communication & Technology, 23(1), pp. 117–123. Available at: https://ejournal.ikmi.ac.id/index.php/jict-ikmi.
Humphreys, E., 2019. Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech house
Imanto, T. (2019) 'Standarisasi_Manajemen_Keamanan_Informas'.
Mahersmi, B. L., Muqtadiroh, F. A., & Hidayanto, B. C. (2016). Analisis risiko keamanan informasi dengan menggunakan metode octave dan kontrol Iso 27001 pada Dishubkominfo Kabupaten Tulungagung. SESINDO 2016, 2016.
Muharni, S. (2021) ANALISA DAN PERANCANGAN SISTEM INFORMASI.
Yogyakarta: CV. Bintang Surya Madani.
N. Hidaya and I. Jatnika, "PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI DATA CENTER STANDART SNI ISOIEC 27001:2013," JUSIM, vol. 7, pp. 24–36, 2022.
Nasution, A. A., & Nasution, M. I. P. (2024). Analisis Keamanan Informasi dalam Sistem Informasi Manajemen: Tantangan dan Solusi di Era Cybersecurity. Journal Of Informatics And Busisnes, 2(2), 168-170.
Ningrum, F. A. S., Riwanto, Y., Pratiwi, I. Y. R., & Fikri, M. A. (2024). Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI. Jurnal Informatika Polinema, 10(3).
Octariza, N. F. (2019). Analisis sistem manajemen keamanan informasi menggunakan standar iso/Iec 27001 dan iso/lec 27002 pada kantor pusat pt jasa mar (Bachelor's thesis, Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta).
Purnama, I., Ritonga, A. A., Pane, R., Bangun, B., & Pratama, R. S. (2021). Perancangan Sistem Informasi Data Bahan-Bahan Material UD. Sinar Baru Sigambal. Journal Computer Science and Information Technology (JCoInT), 2(1), 1-7.
Putrianingsih, S., Muchasan, A., & Syarif, M. (2021). Peran perencanaan pembelajaran terhadap kualitas pengajaran. INOVATIF: Jurnal Penelitian Pendidikan, Agama, Dan Kebudayaan, 7(1), 138-163.
Sandrawati, N.A. (2022) 'Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan Tik Di Kpu', Electoral Governance, 3(2), pp. 232–257.
Sandström, E. and Weiss, J. (2005) 'Cyber security', 2005 CIGRE/IEEE PES International Symposium, pp. 282–289. Available at: https://doi.org/10.1109/CIGRE.2005.1532753.
Saputra, F., Soesanto, E., Cahyaningtyas, K. I., & Hakim, Z. L. (2024). Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo. IJM: Indonesian Journal of Multidisciplinary, 2(1).
Techterms. (2022, agustus 16). Retrieved from Cyberspace Definition: https://techterms.com/definition/cyberspace
Tita, S. (2022). Sistem informasi perpustakaan Sekolah Dasar Negeri 49 Oku menggunakan embarcadero xe2 berbasis client server. JIK: Jurnal Informatika dan Komputer, 13(2), 57-66.
Ys, M. A. F., Zen, B. P., & Wasitarini, D. E. Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. Cyber Security dan Forensik Digital, 6(2), 76-82.