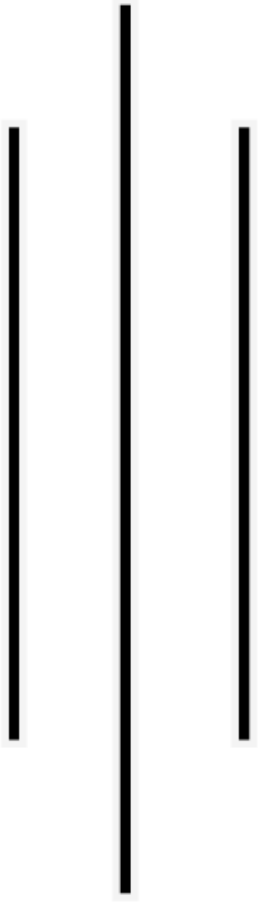
SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)
HANNIE ENTERTAINMENT

(*Versi Dummy untuk Keperluan Portofolio*)



Dokumen SMKI – ISO/IEC 27001:2022

Disusun oleh : Ardhea Oktaviany

Daftar Isi

1. Pendahuluan

Hannie Entertainment, sebagai perusahaan yang bergerak di bidang media dan hiburan digital, menyadari pentingnya menjaga keamanan informasi termasuk informasi pribadi artis, data mitra kerja, data audiens, serta berbagai informasi sensitif lainnya, dalam mendukung kelangsungan bisnis serta membangun kepercayaan mitra dan audiens, khususnya para penggemar artis yang dikelola. Oleh karena itu, Sistem Manajemen Keamanan Informasi (SMKI) dirancang untuk melindungi aset informasi perusahaan dari berbagai risiko, serta memastikan kelangsungan layanan digital yang aman dan terpercaya. (Dokumen ini disusun sebagai bentuk inisiatif mandiri berdasarkan pemahaman dan pengalaman praktis dalam menerapkan prinsip ISO/IEC 27001:2022).

2. Konteks Organiasi

A. Isu Eksternal

Isu eksternal adalah faktor-faktor di luar kendali langsung Hannie Entertainment, namun tetap dapat diantisipasi dan diadaptasi agar tidak mengganggu tujuan strategis perusahaan, terutama dalam menjaga keamanan informasi. Berikut adalah beberapa contoh isu eksternal :

1) Peraturan dan Perundang-undangan yang Berlaku
2) Persepsi dan Nilai-Nilai Pihak Berkepentingan Eksternal
3) Tren dan Inovasi Teknologi
4) Meningkatkan Pengamanan Data dan Informasi

Isu eksternal ini membantu Hannie Entertainment untuk mematuhi klausul 4.2 ISO/IEC 27001:2022, yaitu memahami kebutuhan dan ekspektasi pihak yang berkepentingan dalam hal keamanan informasi.

Isu	Deskripsi	Tantangan	Kesempatan
Peraturan dan Perundang-undangan yang Berlaku	Adanya regulasi nasional yang mengatur keamanan dan perlindungan data, seperti: - UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) - UU No. 28 Tahun 2014 tentang Hak Cipta - UU No. 19 Tahun 2016 tentang	Penyesuaian kebijakan internal agar sesuai dengan regulasi yang berlaku dan terus berkembang, serta memastikan seluruh tim memahami dan menerapkannya.	Meningkatkan kepercayaan publik dan memperkuat citra perusahaan sebagai entitas yang patuh hukum, bertanggung jawab terhadap data pribadi, serta peduli terhadap etika digital.

	Informasi dan Transaksi Elektronik (ITE) - Kebijakan dari platform digital seperti YouTube, Instagram, dan lainnya yang harus dipatuhi oleh perusahaan dalam mengelola konten dan data pengguna.		
Persepsi dan Nilai-Nilai Pihak Berkepentingan	Masyarakat dan mitra makin peduli terhadap transparansi dan keamanan informasi digital artis.	Menjaga kepercayaan publik terhadap integritas Hannie Entertainment.	Meningkatkan loyalitas penggemar dan memperluas kemitraan yang mengutamakan etika digital.
Tren dan Inovasi Teknologi	Perkembangan AI, live streaming, dan cloud-based services membuka peluang sekaligus risiko terhadap keamanan informasi.	Kebutuhan adaptasi teknologi yang cepat dan aman, serta SDM yang siap menghadapi perubahan.	Mendorong inovasi layanan digital dan membangun sistem keamanan yang kompetitif.
Meningkatkan Pengamanan Data dan Informasi	Ancaman seperti peretasan, phishing, dan penyalahgunaan data artis memerlukan kontrol keamanan yang tangguh dan adaptif.	Mendeteksi dan merespons ancaman siber secara proaktif di tengah dinamika digital.	Mengembangkan sistem keamanan informasi yang andal serta meningkatkan kesadaran dan pelatihan keamanan siber secara internal.

B. Isu Internal

Isu internal adalah faktor-faktor yang berasal dari dalam Hannie Entertainment dan berada dalam kendali langsung perusahaan. Faktor-faktor ini perlu dikelola secara efektif agar tidak menghambat pencapaian tujuan strategis, khususnya dalam menjaga keamanan informasi. Berikut adalah beberapa contoh isu internal :

1) Struktur Organisasi
2) Kesadaran dan Kompetensi Personel

3) Standarisasi dan Tata Kelola Teknologi Informasi (TI)
4) Pengelolaan Data dan Informasi

Pengumpulan, penyimpanan, dan distribusi data internal (termasuk kontrak artis, konten eksklusif, dan strategi bisnis) harus dilakukan secara aman dan sesuai prinsip perlindungan informasi.

Isu	Deskripsi	Tantangan	Kesempatan
Struktur Organisasi	Tanggung jawab dan kewenangan dalam pengelolaan informasi harus terstruktur agar tidak terjadi tumpang tindih atau kelalaian, terutama pada data artis dan proyek.	Menyusun struktur dan SOP yang jelas di tengah dinamika industri hiburan yang fleksibel.	Membangun organisasi yang lebih profesional dan terkontrol dalam pengelolaan keamanan informasi.
Kesadaran dan Kompetensi Personel	Karyawan yang belum memahami atau patuh terhadap kebijakan keamanan informasi dapat menjadi titik lemah dalam sistem.	Meningkatkan kesadaran dan pelatihan berkelanjutan di lingkungan kerja yang serba cepat.	Menyelenggarakan pelatihan rutin dan membentuk budaya sadar keamanan informasi.
Standarisasi dan Tata Kelola TI	Ketiadaan prosedur standar seperti backup, enkripsi, dan pengelolaan akses dapat menyebabkan kebocoran atau kehilangan data penting.	Merancang dan menerapkan standar TI yang sesuai dengan kebutuhan operasional tanpa mengganggu kelancaran kerja.	Meningkatkan efisiensi dan keamanan sistem melalui kebijakan dan prosedur TI yang terstandar.
Pengelolaan Data dan Informasi	Data internal seperti kontrak artis, strategi, dan konten harus dikelola dengan aman sesuai prinsip	Memastikan sistem pengelolaan data berjalan aman, efisien, dan sesuai regulasi, terutama dengan data sensitif	Mengembangkan sistem pengelolaan informasi yang komprehensif dan dapat diandalkan sebagai keunggulan

	perlindungan informasi.	berskala besar.	kompetitif perusahaan.

C. Kebutuhan dan Ekspetasi dari Pihak yang Berkepentingan

Pihak-pihak yang berkepentingan terhadap keamanan informasi di Hannie Entertainment memiliki pengaruh dan ekspektasi tertentu yang harus dipahami dan dipenuhi agar tujuan strategis perusahaan tercapai secara aman dan berkelanjutan. Berikut adalah beberapa pihak berkepentingan beserta kebutuhan dan ekspektasinya secara umum :

1) Karyawan
2) Manajemen dan Pemilik Perusahaan
3) Artis dan Talent
4) Penggemar dan Publik
5) Platform Media Sosial dan Mitra Teknologi
6) Regulator dan Pemerintah (mis. Kominfo, BSSN)

Pihak	Kebutuhan	Ekspetasi
Karyawan	Perlindungan data pribadi dan sistem kerja yang aman serta mudah digunakan.	Sistem informasi internal yang aman, efisien, dan mudah digunakan tanpa mengorbankan keamanan data pribadi.
Manajemen dan Pemilik Perusahaan	Pengelolaan risiko keamanan informasi yang efektif untuk menjaga reputasi dan mendukung keberlanjutan bisnis.	Sistem manajemen keamanan informasi yang terstruktur, dapat diaudit, dan mendukung keputusan strategis perusahaan.
Artis dan Talent	Perlindungan atas data pribadi, kontrak kerja, serta aktivitas digital dari ancaman kebocoran dan penyalahgunaan.	Jaminan kerahasiaan informasi pribadi, kontrol akses yang tepat, serta kepercayaan terhadap sistem pengelolaan data digital mereka.
Penggemar dan Publik	Keamanan dalam interaksi digital dan transparansi dalam pengelolaan data yang melibatkan mereka.	Rasa aman dalam berinteraksi dengan platform resmi Hannie Entertainment, serta transparansi dan kepatuhan terhadap regulasi data

		pribadi.
Platform Media Sosial dan Mitra Teknologi	Kepatuhan terhadap kebijakan privasi, integritas data, dan hak cipta selama kerja sama atau pemberian layanan teknologi.	Kolaborasi yang berbasis kepercayaan, dengan implementasi standar keamanan informasi yang diakui dan dipatuhi oleh Hannie Entertainment.
Regulator dan Pemerintah (Kominfo, BSSN)	Penerapan regulasi nasional seperti UU PDP dan standar keamanan informasi (misalnya ISO/IEC 27001:2022).	Kesesuaian dan kepatuhan terhadap kebijakan pemerintah serta kesiapan menghadapi potensi risiko siber secara nasional.

3. Ruang Lingkup SMKI

Ruang lingkup sertifikasi penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar internasional ISO/IEC 27001:2022 adalah : Sistem Manajemen Keamanan Informasi untuk pengelolaan, perlindungan, dan pemeliharaan data digital, aset informasi, serta infrastruktur teknologi yang digunakan dalam kegiatan operasional Hannie Entertainment, termasuk manajemen artis, distribusi konten digital, dan interaksi dengan mitra serta publik.

A. Keterhubungan dan Dependensi

No	Aspek	Keterhubungan	Dependensi
1.	Proses Bisnis	Proses pengelolaan data artis, kontrak kerja, dan proyek dilakukan oleh tim internal untuk mendukung operasional manajemen dan produksi.	Vendor sebagai pengembang sistem manajemen proyek yang digunakan oleh Hannie Entertainment, atau pengelolaan dilakukan oleh tim internal TI.
2.	Sumber Daya Manusia	Pengelolaan data dan akses informasi karyawan, artis, serta kru dilakukan melalui sistem HR yang terhubung dengan direktorat kepegawaian.	Ketergantungan pada sistem HR digital dan pelatihan SDM dalam menjaga keamanan akses serta autentikasi pengguna internal.
3.	Fasilitas Pendukung	Sistem keamanan informasi didukung oleh perangkat	Bergantung pada ketersediaan layanan

		keras (server, storage, CCTV, access control) yang terintegrasi dengan sistem pusat perusahaan.	fasilitas seperti daya listrik, jaringan internet, serta vendor pemeliharaan perangkat keras dan lunak.
4.	Lokasi	Seluruh kantor dan studio Hannie Entertainment memiliki sistem keamanan informasi yang saling terhubung melalui jaringan intranet dan VPN.	Ketergantungan pada konektivitas jaringan antar lokasi dan kesiapan site recovery plan untuk memastikan kelangsungan operasional jika terjadi gangguan.

4. Kepemimpinan

A. Kepemimpinan dan Komitmen

Hannie Entertainment menunjukkan kepemimpinan dan komitmen dalam implementasi Sistem Manajemen Keamanan Informasi (SMKI), melalui langkah-langkah berikut :

1) Memastikan kebijakan dan tujuan SMKI selaras dengan visi dan misi Hannie Entertainment dalam menyediakan layanan hiburan yang profesional, aman, dan berbasis teknologi informasi;
2) Memastikan integrasi persyaratan SMKI ke dalam proses bisnis inti, manajemen artis, produksi konten, serta aktivitas pendukung lainnya;
3) Menyediakan sumber daya yang memadai, termasuk personel, infrastruktur teknologi, dan anggaran, untuk mendukung keberhasilan implementasi SMKI;
4) Mengkomunikasikan pentingnya penerapan SMKI secara efektif dan konsisten kepada seluruh karyawan, mitra, dan pihak terkait;
5) Menjamin pencapaian hasil SMKI yang sesuai dengan harapan perusahaan dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi artis, proyek, dan data perusahaan;
6) Mendorong dan memfasilitasi partisipasi aktif dari seluruh staf dan tim produksi dalam mendukung keberhasilan dan efektivitas SMKI;
7) Mendukung perbaikan berkelanjutan dalam semua aspek manajemen keamanan informasi di seluruh unit organisasi;
8) Memberikan mandat dan dukungan kepada setiap kepala unit/divisi untuk menjalankan kepemimpinan yang bertanggung jawab terhadap keamanan informasi di area kerjanya masing-masing.

B. Kebijakan

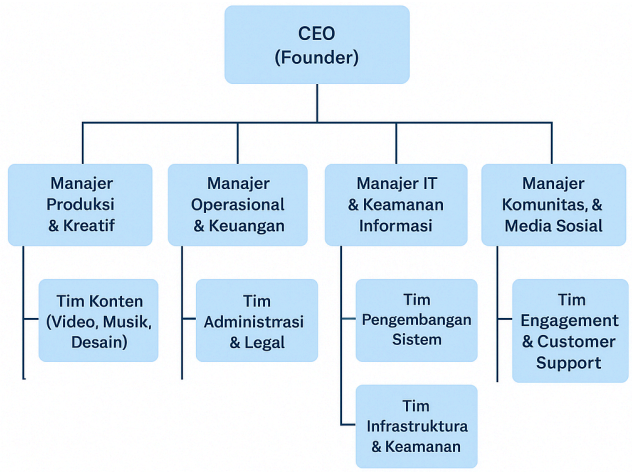
Hannie Entertainment berkomitmen untuk mengelola dan melindungi informasi secara aman, terstruktur, dan berkelanjutan, sesuai dengan kebutuhan industri hiburan

dan multimedia. Kebijakan ini disusun dengan mengacu pada regulasi nasional yang berlaku, termasuk Undang-Undang Perlindungan Data Pribadi dan hukum terkait hak kekayaan intelektual. Komitmen kebijakan SMKI Hannie Entertainment mencakup :

1) Melindungi informasi penting perusahaan, termasuk data artis, kontrak, dan proyek, dengan menjamin Kerahasiaan, Integritas, dan Ketersediaan informasi melalui penerapan standar ISO/IEC 27001:2022;
2) Mematuhi seluruh peraturan perundang-undangan yang berlaku di Indonesia, serta kebijakan industri hiburan terkait keamanan informasi dan privasi;
3) Melaksanakan peningkatan berkelanjutan terhadap kinerja SMKI, agar sistem informasi perusahaan senantiasa andal, aman, dan siap menghadapi perubahan teknologi serta ancaman siber.

Kebijakan ini ditetapkan oleh manajemen puncak, didokumentasikan, dikomunikasikan kepada seluruh pemangku kepentingan, dan akan ditinjau secara berkala setidaknya sekali dalam satu tahun. Kebijakan ini bersifat terbuka dan dapat diakses oleh pihak internal maupun eksternal yang berkepentingan.

C. Peran, Tanggung Jawab, dan Otoritas Organisasi SMKI



Peran SMKI	Nama Peran	Peran	Tanggung Jawab	Otoritas
Top Management	CEO (Founder)	Kepemimpinan puncak dalam SMKI	1. Menetapkan dan mengesahkan Kebijakan SMKI 2. Menyediakan sumber daya (anggaran, SDM,	1. Memulai /menghentikan implementasi SMKI 2. Mengangkat /memberhentikan Koordinator SMKI

			infrastruktur) 3. Menyetujui sasaran dan rencana SMKI	3. Mengangkat Internal Auditor 4. Menyetujui alokasi anggaran SMKI
Koordinator SMKI	Manajer IT & Keamanan Informasi	Koordinasi keseluruhan implementasi SMKI	1. Menyusun rencana dan jadwal SMKI 2. Memantau pelaksanaan dan pelaporan ke Top Management 3. Mengelola pertemuan organisasi SMKI a. Mengakses seluruh dokumentasi SMKI b. Mengusulkan penunjukan tim pelaksana c. Menghentikan kegiatan yang tidak sesuai SMKI	1. Mengakses seluruh dokumentasi SMKI 2. Mengusulkan penunjukan tim pelaksana 3. Menghentikan kegiatan yang tidak sesuai SMKI
Koordinator Aset	Manajer Produksi & Kreatif	Pengelolaan aset informasi	1. Mengidentifikasi dan mendata aset informasi 2. Menilai nilai dan risiko aset 3. Mengusulkan kontrol teknis dan organisatoris pada aset a. Menyetujui klasifikasi dan penanganan aset b. Mengelola akses ke aset informasi	1. Menyetujui klasifikasi dan penanganan aset 2. Mengelola akses ke aset informasi
Koordinator Risiko	Manajer Operasional & Keuangan	Manajemen risiko SMKI	1. Melakukan identifikasi, analisis, dan evaluasi risiko 2. Merancang dan	1. Menetapkan risk appetite 2. Menyetujui penanganan risiko 3. Menghentikan

			memantau tindakan mitigasi 3. Memelihara Risk Register	aktivitas berisiko tinggi
Koordinator SDM	Manajer Komunitas & Media Sosial	Kesadaran & pelatihan SMKI	1. Menyusun dan melaksanakan program sosialisasi 2. Mengadakan pelatihan dan simulasi keamanan informasi 3. Memonitor efektivitas pelatihan	1. Menetapkan materi dan jadwal pelatihan 2. Mengalokasikan anggaran untuk awareness
Koordinator Dokumentasi	Tim Administrasi & Legal	Pengelolaan dokumentasi SMKI	1. Mengontrol versi dan distribusi dokumen 2. Memelihara catatan (record) SMKI 3. Menyiapkan template dan prosedur dokumentasi	1. Mengedit, menambah, atau menarik dokumen SMKI 2. Menetapkan retensi dan aksesibilitas dokumen
Internal Auditor	Auditor Internal	Melakukan audit internal SMKI	1. Menyusun rencana dan program audit 2. Melakukan audit sesuai kriteria ISO 27001 3. Melaporkan temuan dan rekomendasi perbaikan	1. Akses penuh ke semua area dan catatan SMKI 2. Merekomendasikan tindakan korektif dan pencegahan
Tim Tanggap Insiden	Tim Infrastruktur & Keamanan	Respon dan penanganan insiden keamanan	1. Mendeteksi dan menangani insiden 2. Menyusun laporan dan root cause analysis insiden 3. Melakukan evaluasi pasca-insiden	1. Mengisolasi atau memulihkan sistem 2. Melakukan tindakan darurat tanpa persetujuan tingkat atas

Tim BCP	Tim Pengembangan Sistem	Perencanaan & pengujian Business Continuity	1. Menyusun dan memperbarui rencana kontinuitas bisnis 2. Melakukan uji coba (drill) BCP 3. Memelihara dokumentasi pemulihan	1. Mengaktifkan rencana BCP dalam keadaan darurat 2. Mengkoordinasi sumber daya lintas unit
Data Privacy Officer	Bagian Legal (Data Privacy)	Kepatuhan perlindungan data pribadi	1. Menilai dampak privasi (DPIA) 2. Menangani permintaan hak subjek data 3. Melakukan audit kepatuhan UU PDP	1. Menghentikan pemrosesan data yang melanggar peraturan 2. Mengeluarkan dan menegakkan kebijakan privasi

5. Perencanaan

A. Tindakan untuk Mengatasi Risiko dan Peluang

Hannie Entertainment menyiapkan dokumen Metodologi Risiko sebagai pedoman untuk :

1) Mengidentifikasi risiko dan peluang yang berkaitan dengan keamanan informasi, serta merencanakan langkah-langkah mitigasi atau penguatan yang diperlukan;
2) Mengintegrasikan dan mengimplementasikan tindak lanjut dari hasil penilaian risiko ke dalam berbagai proses dalam Sistem Manajemen Keamanan Informasi (SMKI), dan mengevaluasi efektivitas tindakan yang telah dilakukan.

Langkah-langkah dalam melakukan Penilaian Risiko Keamanan Informasi di Hannie Entertainment adalah sebagai berikut :

1) Identifikasi Risiko
   Mengumpulkan dan mendata potensi risiko yang dapat mengancam keamanan informasi perusahaan, baik dari aspek internal maupun eksternal;
2) Analisis dan Perhitungan Risiko
   Melakukan analisis dampak dan kemungkinan terjadinya risiko, serta menentukan level risiko berdasarkan parameter yang telah ditentukan;
3) Menentukan Risk Appetite
   Menetapkan tingkat risiko yang dapat diterima oleh manajemen Hannie Entertainment sebagai dasar pengambilan keputusan dalam pengelolaan risiko;
4) Penanganan Risiko
   Menyusun strategi dan tindakan mitigasi terhadap risiko yang tidak dapat diterima, serta memastikan tindakan tersebut diimplementasikan secara efektif.

B. Objektif Keamanan Informasi

Adapun sasaran yang ingin dicapai dalam pelaksanaan SMKI di Hannie Entertainment adalah sebagai berikut :

No	Sasaran	Target	PIC
1.	Melakukan Awareness SMKI	1 kali dalam satu tahun	Tim Keamanan Informasi
2.	Melakukan penetration test pada aplikasi dan infrastruktur pendukung serta melakukan perbaikan	2 kali dalam satu tahun	Tim Keamanan Informasi
3.	Melakukan vulnerability assessment	Setiap 3 bulan	Tim Keamanan Informasi
4.	Melakukan internal audit	Min 1 kali dalam satu tahun	Auditor Internal
5.	Melakukan manajemen review	Min 1 kali dalam satu tahun	Auditor Internal, Tim Keamanan Informasi, Tim Infrastruktur dan Inovasi
6.	Melakukan server dan network hardening review sesuai standar keamanan	80% Passed	Tim Infrastruktur dan Teknisi

6. Dukungan

A. Sumber Daya

Hannie Entertainment menetapkan dan menyediakan sumber daya yang diperlukan untuk persiapan, implementasi, pemeliharaan, dan peningkatan berkelanjutan Sistem Manajemen Keamanan Informasi (SMKI) sesuai ruang lingkup perusahaan.

1) Anggaran

Hannie Entertainment mengalokasikan anggaran khusus untuk pengembangan dan penguatan SMKI, termasuk investasi dalam perangkat lunak keamanan, sistem penyimpanan data, dan peningkatan infrastruktur digital.

2) Sumber Daya Manusia

Manajemen menunjuk personel dari unit IT & Keamanan Informasi yang bertanggung jawab terhadap pengelolaan dan pengawasan SMKI secara

menyeluruh, dengan dukungan kolaboratif dari unit terkait lainnya seperti tim legal dan manajemen proyek.

B. Kompetensi

Manajemen menunjuk personel dari unit IT & Keamanan Informasi yang bertanggung jawab terhadap pengelolaan dan pengawasan SMKI secara menyeluruh, dengan dukungan kolaboratif dari unit terkait lainnya seperti tim legal dan manajemen proyek.

C. Kesadaran

1) Seluruh staf Hannie Entertainment, terutama yang terlibat dalam pengelolaan data digital artis, proyek, dan pelanggan, wajib mendapatkan sosialisasi rutin mengenai keamanan informasi yang diterapkan di perusahaan.
2) Semua staf diharapkan untuk :
    a. Mengetahui, memahami, dan menjalankan kebijakan keamanan informasi yang berlaku;
    b. Berkontribusi aktif dalam pelaksanaan dan perbaikan berkelanjutan SMKI guna menjaga keberlangsungan bisnis;
    c. Menyadari risiko dan konsekuensi dari pelanggaran atau ketidaksesuaian terhadap kebijakan SMKI.

Manajemen Hannie Entertainment menyelenggarakan program sosialisasi dan pelatihan internal untuk menumbuhkan kesadaran akan :

1) Pentingnya implementasi kebijakan keamanan informasi dalam menjaga reputasi dan integritas perusahaan;
2) Peran aktif seluruh staf dalam menjaga efektivitas dan kesuksesan sistem manajemen keamanan informasi;
3) Implikasi dari ketidakpatuhan terhadap SMKI, seperti terjadinya kebocoran data, pelanggaran hukum, atau hilangnya kepercayaan publik.

D. Rencana Komunikasi

Hannie Entertainment berkomunikasi dengan pihak internal dan eksternal terkait implementasi SMKI yang mencakup :

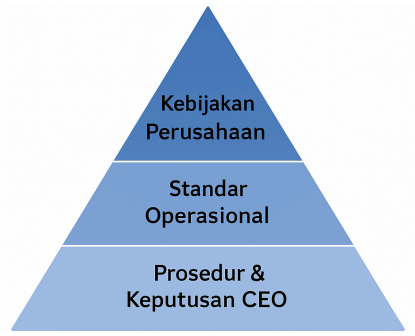
No.	Agenda Komunikasi	Periode	Pihak yang Dikomunikasikan	PIC	Metode Komunikasi
1.	Management Review	Tahunan	Internal	Manajer IT & Keamanan	Rapat

				Informasi	
2.	Sosialiasi/Awareness SMKI	Tahunan	Internal, Eksternal	Tim Infrastruktur & Keamanan	Rapat, email, poster digital
3.	Diskusi Isu Keamanan Informasi dengan Regulator	Situasional /sesuai kebutuhan	Internal, Eksternal	Tim Legal, Tim IT	Rapat, online meeting, mobile phone
4.	Permintaan perubahan/penambahan sistem atau kebijakan	Sesuai kebutuhan	Internal, Eksternal	Tim Pengembangan Sistem	Laporan tertulis, email
5.	Pelaporan pencapaian kinerja SMKI	Sesuai kebutuhan	Internal, Eksternal	Manajer IT & Keamanan Informasi	Rapat, dokumentasi laporan
6.	Pelaporan hasil audit sistem & pengujian keamanan digital	Sesuai kebutuhan	Internal	Tim Keamanan Informasi	Rapat, laporan berkala

E. Dokumentasi Informasi SMKI

1) Kontrol Dokumentasi

Hierarki dan pengaturan dokumentasi SMKI yang diterapkan di Hannie Entertainment disusun dalam tingkatan sebagai berikut :



Kontrol dokumen informasi dibuat dan dipelihara untuk tujuan :

a. Memberikan bukti kesesuaian dengan persyaratan dan efektivitas operasional dari SMKI;

b. Digunakan sebagai bukti pelaksanaan, materi analisis data, memastikan proses kesesuaian, dan sebagai bahan pengukuran efektivitas implementasi SMKI;
c. Catatan/model selalu terbaca, dapat diidentifikasi dengan mudah, dan siap diambil saat dibutuhkan;
d. Menetapkan mekanisme kontrol, pengambilan, lama retensi, dan catatan distribusi informasi untuk seluruh dokumen penting terkait keamanan informasi.

Proses kontrol lengkap terhadap dokumen mengacu pada Pedoman Penyusunan dan Pengelolaan Dokumen Internal Hannie Entertainment.

2) Persiapan dan Pengkinian Dokumen

Dalam penyusunan dan pengkinian dokumen informasi SMKI, Manajemen Hannie Entertainment menetapkan persyaratan sebagai berikut :

a. Identifikasi jenis dokumen dan deskripsi yang dibutuhkan sesuai dengan ruang lingkup keamanan informasi perusahaan;
b. Penetapan format isi dokumen, struktur penulisan, serta media penyimpanan (fisik maupun digital);
c. Adanya proses peninjauan berkala dan persetujuan dari pihak terkait untuk memastikan kelayakan, keakuratan, dan relevansi dokumen terhadap kondisi terkini.

Proses penyusunan dan pemutakhiran dokumen mengacu pada Pedoman Penyusunan dan Pengelolaan Dokumen Keamanan Informasi Hannie Entertainment.

7. Operasional

A. Perencanaan dan Kontrol Operasional

Manajemen Hannie Entertainment merencanakan, melaksanakan, dan mengendalikan proses yang diperlukan untuk memenuhi persyaratan standar, serta untuk melaksanakan tindak lanjut yang ditentukan melalui :

Aktivitas	Detail Aktivitas	Agenda Tahunan	Pihak yang Berkaitan
Vulnerability Assessment dan Penetration Testing	a. Melakukan pengujian terhadap infrastruktur TI b. Melakukan pengujian keamanan terhadap aplikasi internal dan	Q2	Manajer IT & Keamanan Informasi

	eksternal		
Analisis dan Penilaian Risiko	a. Pembaruan identifikasi aset/proses b. Pembaruan identifikasi risiko c. Memperbarui rencana pengendalian risiko	Q2	Koordinator Risiko (bisa dari fungsi IT/Legal)
Peningkatan Kompetensi SDM	a. Pelatihan terkait peningkatan kompetensi keamanan informasi b. Sosialisasi peningkatan kesadaran keamanan digital bagi seluruh karyawan	Sepanjang Tahun	Koordinator SDM / Manajer Operasional
Audit Internal	a. Penyusunan rencana/program audit b. *Kickoff*/penutupan audit internal c. Pelaksanaan audit sesuai kriteria SMKI dan ISO 27001	Q2	Auditor Internal (ditunjuk Manajemen)
Review Manajemen	a. Pemaparan hasil rapat Review Manajemen sebelumnya b. Menindaklanjuti hasil audit internal c. Rencana tindak lanjut risiko d. Isu terkini terkait keamanan informasi	Q2	Top Management, Organisasi SMKI

Audit Eksternal	a. Rencana/program audit b. Implementasi audit dari pihak ketiga	Q2	Top Management, Organisasi SMKI

B. Penilaian Risiko

Dalam penilaian risiko pada Hannie Entertainment, langkah pertama yang dilakukan adalah Identifikasi Risiko, dengan cara :

1) Mengidentifikasi aset informasi dalam lingkup Sistem Manajemen Keamanan Informasi (SMKI), sesuai dengan dokumen Daftar Aset Informasi Hannie Entertainment.
2) Mengidentifikasi kerentanan (vulnerability) yang terdapat pada aset tersebut;
3) Mengidentifikasi ancaman (threat) yang mungkin terjadi akibat kerentanan tersebut terhadap aset;
4) Mengidentifikasi dampak (impact) yang dapat menggambarkan potensi kerugian, baik dari sisi kerahasiaan, integritas, maupun ketersediaan aset informasi yang dimiliki oleh Hannie Entertainment.

C. Penanganan Risiko

Setelah proses identifikasi dan penilaian risiko dilakukan, Hannie Entertainment akan melakukan penanganan risiko untuk memastikan setiap risiko dikelola secara efektif. Langkah-langkah penanganan risiko meliputi :

1) Evaluasi Risiko

   Menentukan tingkat risiko berdasarkan kemungkinan terjadinya dan tingkat dampaknya terhadap operasi Hannie Entertainment. Risiko dikategorikan ke dalam tingkat (tinggi, sedang, rendah) untuk menentukan prioritas penanganan.
2) Pilihan Penanganan Risiko

   Setiap risiko yang telah dievaluasi akan ditangani melalui salah satu atau kombinasi dari pendekatan berikut :
   a. Menghindari risiko : Menghentikan aktivitas atau proses yang menimbulkan risiko signifikan.
   b. Mengurangi risiko : Menerapkan kontrol keamanan untuk menurunkan kemungkinan terjadinya atau dampaknya.
   c. Menerima risiko : Jika tingkat risikonya rendah atau biaya pengendaliannya terlalu tinggi, risiko dapat diterima dengan dokumentasi persetujuan dari manajemen.
   d. Mentransfer risiko : Memindahkan risiko ke pihak ketiga, seperti melalui asuransi atau perjanjian kerja sama.

3) Implementasi Pengendalian
   Mengimplementasikan kontrol keamanan teknis dan non-teknis yang dirancang untuk menurunkan risiko ke tingkat yang dapat diterima. Misalnya :
   a. Pengamanan akses sistem internal artis dan tim kreatif;
   b. Audit berkala sistem IT;
   c. Proteksi data fans dan pelanggan di platform digital.
4) Pemantauan dan Tinjauan Ulang
   Risiko yang telah ditangani tetap dipantau secara berkala oleh Tim Keamanan Informasi Hannie Entertainment untuk menilai efektivitas pengendalian dan mengidentifikasi potensi risiko baru.

8. Evaluasi Performa

A. *Monitoring*, Pengukuran, Analisis dan Evaluasi
   Kegiatan Monitoring, Pengukuran, Analisis, dan Evaluasi terhadap Sistem Manajemen Keamanan Informasi (SMKI) di Hannie Entertainment dilakukan melalui langkah-langkah berikut :
   1) Menetapkan, Memelihara, dan Mengontrol SMKI dengan cara :
      a. Mendeteksi proses yang sedang berjalan ketika terjadi penyimpangan dalam sistem produksi, distribusi konten, atau operasional, dan segera menindaklanjuti sesuai dengan prosedur yang ditetapkan oleh manajemen.
      b. Seluruh pengguna sistem (tim kreatif, produksi, pemasaran, IT, dan lainnya) bertanggung jawab untuk menjaga kerahasiaan data internal perusahaan dan informasi sensitif lainnya, serta mematuhi kebijakan dan prosedur keamanan informasi yang berlaku di Hannie Entertainment.
      c. Mengevaluasi langkah-langkah penanganan yang berkaitan dengan pelanggaran keamanan informasi dalam operasional harian (misalnya kebocoran data konten sebelum perilisan), serta memastikan adanya transparansi dan akuntabilitas dalam pelaporan insiden.
      d. Mengevaluasi efektivitas tindakan korektif yang telah diambil setelah terjadinya insiden keamanan untuk memastikan tidak terulangnya kejadian serupa di masa mendatang.

   2) Kajian Terhadap Risk Register
      Risk Register SMKI dikaji setidaknya satu kali dalam setahun, dengan mempertimbangkan :
      a. Perkembangan teknologi yang digunakan oleh Hannie Entertainment dalam produksi, distribusi, dan promosi konten digital;
      b. Perubahan dalam proses bisnis dan kerja sama industri (misalnya kontrak dengan platform streaming, agensi luar negeri, atau sponsor);

c. Ancaman keamanan informasi yang baru muncul (termasuk serangan siber, pencurian konten, dll);
d. Efektivitas pengendalian yang telah diterapkan sebelumnya;
e. Faktor eksternal seperti perubahan regulasi industri hiburan, hak cipta, dan teknologi media sosial.

B. Audit Internal

Tata cara pelaksanaan Audit Internal SMKI di Hannie Entertainment diatur dalam Framework Internal Audit, Sistem Review Manajemen, dan Perbaikan Berkelanjutan, dengan mekanisme sebagai berikut :

1) Audit internal dilakukan minimal satu kali dalam setahun untuk mengevaluasi pencapaian tujuan bisnis, kinerja operasional, proses keamanan informasi, serta kepatuhan terhadap kebijakan internal perusahaan dan standar industri hiburan yang berlaku.
2) Tim audit ditunjuk langsung oleh CEO atau Manajer Operasional melalui Surat Tugas Resmi. Anggota tim audit dapat berasal dari staf internal perusahaan, seperti tim IT, keuangan, atau manajemen risiko. Auditor harus memiliki kompetensi yang memadai dan memastikan objektivitas serta imparsialitas, dan tidak boleh mengaudit unit yang berada di bawah pengelolaan langsungnya.
3) Hasil audit internal menjadi masukan penting untuk proses evaluasi dan pengambilan keputusan strategis perusahaan. Setiap ketidaksesuaian atau temuan selama audit harus segera ditindaklanjuti oleh unit terkait dan dijadikan dasar perbaikan berkelanjutan.
4) Seluruh catatan, temuan, dan rekomendasi audit harus disimpan secara terdokumentasi dan mudah diakses oleh manajemen untuk kepentingan pelacakan, transparansi, dan akuntabilitas.
5) Program audit disusun berdasarkan sistem manajemen informasi dan operasional yang diterapkan oleh Hannie Entertainment, termasuk perlindungan terhadap konten digital, data pelanggan, dan aset intelektual perusahaan. Program ini harus mempertimbangkan kebutuhan spesifik perusahaan serta ruang lingkup audit yang ditetapkan manajemen.
6) Pelaksanaan audit dapat menggunakan metode wawancara, observasi lapangan, analisis data, dan dokumen. Audit juga dapat melibatkan stakeholder internal seperti tim produksi, kreatif, pemasaran, hingga mitra teknologi jika relevan.
7) Setelah audit selesai, hasil audit dianalisis untuk mengidentifikasi area yang perlu diperbaiki. Seluruh tindak lanjut dari hasil audit harus dilaporkan kepada manajemen dan menjadi bagian dari rencana perbaikan berkelanjutan perusahaan.

C. Tinjauan Manajemen

Perwakilan Manajemen Hannie Entertainment melakukan tinjauan terhadap Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan framework internal audit, sistem review manajemen, dan prinsip perbaikan berkelanjutan. Tinjauan manajemen ini dilaksanakan secara berkala, minimal satu kali dalam setahun, untuk memastikan bahwa SMKI tetap relevan, lengkap, dan efektif dalam mendukung tujuan strategis perusahaan, terutama dalam melindungi aset digital dan informasi sensitif perusahaan.

Tujuan utama dari tinjauan ini adalah untuk mengevaluasi kesesuaian, kelengkapan, dan efektivitas penerapan SMKI di lingkungan Hannie Entertainment, guna menjaga keamanan data, konten, dan informasi operasional yang digunakan dalam industri hiburan dan media.

Masukan yang menjadi bahan pertimbangan dalam tinjauan manajemen meliputi :

1) Status dan hasil tindak lanjut dari tinjauan manajemen sebelumnya;
2) Perubahan kondisi eksternal dan internal yang berdampak pada SMKI (termasuk teknologi baru, peraturan industri, atau dinamika pasar hiburan);
3) Evaluasi kinerja keamanan informasi dalam operasional perusahaan;
4) Tanggapan atau masukan dari stakeholder internal maupun eksternal;
5) Hasil penilaian risiko dan status implementasi dari rencana penanganan risiko;
6) Tantangan dan peluang yang muncul dari penggunaan teknologi hiburan dan distribusi digital;
7) Tingkat kepatuhan terhadap kebijakan perlindungan data pelanggan, artis, dan mitra;
8) Inisiatif, inovasi, serta rencana peningkatan berkelanjutan dalam pengelolaan keamanan informasi.

9. Peningkatan Berkelanjutan

A. *Non Conformity & Corrective Action*

Apabila terjadi insiden ketidaksesuaian terhadap standar yang diterapkan di Hannie Entertainment, maka perusahaan akan segera mengambil tindakan perbaikan (corrective action) untuk mengendalikan dan menyesuaikan kembali proses yang terdampak agar sesuai dengan kebijakan dan standar yang berlaku. Tindakan korektif yang dilakukan bertujuan untuk mencegah terulangnya insiden serupa, dan didasarkan pada :

1) Laporan insiden keamanan informasi atau gangguan sistem;
2) Temuan dari audit internal maupun eksternal;
3) Hasil Root Cause Analysis (RCA) terhadap penyebab utama ketidaksesuaian;
4) Keputusan dan rekomendasi hasil dari tinjauan manajemen.

Langkah-langkah dalam pelaksanaan tindakan korektif :

1) Mengidentifikasi ketidaksesuaian (non-conformity) terhadap kebijakan, prosedur, atau standar keamanan informasi;
2) Menentukan akar penyebab dari ketidaksesuaian yang terjadi;
3) Mengevaluasi perlunya tindakan untuk mencegah ketidaksesuaian terulang kembali;
4) Merancang dan melaksanakan tindakan korektif yang sesuai dengan skala dan dampak insiden;
5) Melakukan pemantauan dan pengukuran terhadap hasil dari tindakan korektif tersebut;
6) Melakukan evaluasi ulang atas efektivitas tindakan korektif guna memastikan bahwa masalah telah diselesaikan secara menyeluruh.

B. *Continous Improvement*

Dalam rangka meningkatkan efektivitas Sistem Manajemen Keamanan Informasi (SMKI) secara berkelanjutan, manajemen Hannie Entertainment melakukan tinjauan berkala terhadap pencapaian kinerja, kebijakan, sasaran keamanan informasi, serta hasil audit internal maupun eksternal.

Setiap hasil keputusan yang diambil selama proses Review Manajemen harus segera ditindaklanjuti, dan setiap action plan yang telah disusun akan dipantau status pelaksanaannya. Perkembangan dari tindakan perbaikan atau peningkatan tersebut akan menjadi bagian penting dalam agenda tinjauan manajemen berikutnya, guna memastikan bahwa perbaikan terus-menerus (continuous improvement) diterapkan secara konsisten dan berdampak nyata terhadap peningkatan sistem keamanan informasi di seluruh lini operasional Hannie Entertainment.

10. Kepatuhan

No.	Nama Peraturan Eksternal	No/Bab/Pasal Terkait	Status Adopsi dan Keterangan
1.	Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)	a. Bab VII (Pasal 40-42) b. Bab IX (Pasal 50-52) c. Pasal 15	Sudah diadopsi dalam Kebijakan, SOP, dan standar internal terkait sistem manajemen keamanan informasi di Hannie Entertainment

2.	Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)	a. Bab IV (Pasal 16–25) b. Bab V (Pasal 26–43) c. Bab VII–VIII (47–61)	Dalam proses harmonisasi ke dalam kebijakan internal privasi dan pengelolaan data pribadi di Hannie Entertainment
3.	Peraturan Sekretaris Jenderal Kemendikbudristek No. 3 Tahun 2024 tentang Klasifikasi Data	a. Bab II (Klasifikasi Data) b. Bab IV	Dalam perencanaan untuk diadopsi dalam kebijakan klasifikasi data internal dan pengendalian akses berbasis peran

Catatan :

Dokumen ini disusun sebagai bagian dari portofolio simulasi penerapan ISO/IEC 27001:2022.
Tidak merepresentasikan kebijakan resmi suatu entitas hukum tertentu.
Segala isi bersifat fiktif dan bertujuan edukatif.