MANAJEMEN RISIKO KEAMANAN INFORMASI
DI SEKOLAH TINGGI MULTI MEDIA

Nomor Dokumen : SK Ketua STMM No 355 Tahun 2025
Tanggal Terbit : 17 November 2025
Nomor Revisi : 00
Status : Aktif

Tim Penyusun:

Pembina : Dr. R.M. Agung Harimurti (Ketua)
Pengarah : RB. Hendri Kuswantoro, S.Kom, M.Kom (Pembantu Ketua II)
Redaktur : Candra Santosa, S.T, M.Eng (Kepala Unit TIK)
Sekretaris : Purbandaru Pandhu Utami, S.Kom, M.Eng
Anggota : Gusanwar, S.Kom, M.Eng

KEMENTERIAN KOMUNIKASI DAN DIGITAL RI
SEKOLAH TINGGI MULTI MEDIA
Alamat : Jl. Magelang Km. 6 Yogyakarta 55284 INDONESIA Fax : (0274) 586561, 623537, 623460
Telepon : Ketua (0274) 586512 E-mail : Info@mmtc.ac.id
(0274) 561531, 562513, 623537, 7474201

KEPUTUSAN
KETUA SEKOLAH TINGGI MULTI MEDIA
NOMOR 355 TAHUN 2025

TENTANG

MANAJEMEN RISIKO KEAMANAN INFORMASI
DI LINGKUNGAN SEKOLAH TINGGI MULTI MEDIA

KETUA SEKOLAH TINGGI MULTI MEDIA**,**

Menimbang :

a. bahwa dalam rangka mengidentifikasi risiko terkait keamanan informasi yang mungkin terjadi di lingkungan Sekolah Tinggi Multi Media;
b. bahwa diperlukan perencanaan pengendalian risiko keamanan informasi untuk menangani dan mengeliminasi risiko;
c. bahwa diperlukan upaya untuk meningkatkan efektivitas dan pelaksanaan manajemen risiko yang berkelanjutan;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, b, dan c, perlu menetapkan Keputusan Ketua Sekolah Tinggi Multi Media tentang Manajemen Risiko Keamanan Informasi di Lingkungan Sekolah Tinggi Multi Media.

Mengingat :

1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 4301);
2. Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 127, Tambahan Lembaran Negara Nomor 4890);
3. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 16, Tambahan Lembaran Negara Republik Indonesia Nomor 5500);
4. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

5. Peraturan Presiden Republik Indonesia Nomor 33 Tahun 2014 tentang Pendirian Sekolah Tinggi Multi Media (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 82);
6. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 29 Tahun 2014 tentang Organisasi dan Tata Kerja Sekolah Tinggi Multi Media (Berita Negara Republik Indonesia Tahun 2014 Nomor 1278);
7. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 37 Tahun 2014 tentang Statuta Sekolah Tinggi Multi Media (Berita Negara Republik Indonesia Tahun 2014 Nomor 1480);
8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 Tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
9. Peraturan Menteri Komunikasi dan Digital Nomor 1 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Digital (Berita Negara Republik Indonesia Tahun 2025 Nomor 17);
10. Pedoman Menteri Komunikasi dan Informatika Nomor 06 Tahun 2017 tentang Manajemen Risiko di Lingkungan Kementerian Komunikasi dan Informatika;
11. Pedoman Menteri Komunikasi dan Informatika Nomor 03 Tahun 2018 Tentang Klasifikasi Arsip Di Lingkungan Kementerian Komunikasi dan Informatika;
12. Pedoman Menteri Komunikasi dan Informatika Nomor Tahun 03 Tahun 2019 Tentang Tata Naskah Dinas di Lingkungan Kementerian Komunikasi dan Informatika;
13. Surat Keputusan Sekretariat Jenderal Kementerian Komunikasi dan Informatika Nomor 72 Tahun 2023 tentang Standar Sistem Keamanan Informasi di Lingkungan Kementerian Komunikasi dan Informatika;
14. ISO 31000:2018 Risk Management Awareness;
15. ISO/IEC 27005:2018 Information Security Risk Management.

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KETUA SEKOLAH TINGGI MULTI MEDIA TENTANG MANAJEMEN RISIKO KEAMANAN INFORMASI DI LINGKUNGAN SEKOLAH TINGGI MULTI MEDIA.

KESATU : Menetapkan Manajemen Risiko Keamanan Informasi di Lingkungan Sekolah Tinggi Multi Media sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini;

KEDUA : Kebijakan Manajemen Risiko Keamanan Informasi di Lingkungan Sekolah Tinggi Multi Media sebagaimana dimaksud pada Diktum KESATU berlaku untuk aset informasi yang dikelola atau milik Sekolah Tinggi Multi Media;

KETIGA : Kebijakan Manajemen Risiko Keamanan Informasi di Lingkungan Sekolah Tinggi Multi Media bertujuan untuk mengidentifikasi dan meminimalkan kemungkinan risiko keamanan informasi di Sekolah Tinggi Multi Media;

KEEMPAT : Keputusan ini berlaku sejak tanggal ditetapkan dengan ketentuan apabila dikemudian hari terdapat kekeliruan dalam penetapan ini akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Yogyakarta
Pada tanggal 17 November 2025

KETUA,

No	Nama	Jabatan	Paraf
1.	RB Hendri K	Puket II	
2.	Candra S	Kanit TIK	
3.	Triawan S	Ketua SPI	

R.M. AGUNG HARIMURTI

LAMPIRAN I
KEPUTUSAN KETUA SEKOLAH TINGGI MULTI MEDIA
NOMOR 355 TAHUN 2025
TENTANG
MANAJEMEN RISIKO KEAMANAN INFORMASI DI LINGKUNGAN SEKOLAH TINGGI MULTI MEDIA

A. Latar Belakang

Dalam era transformasi digital, informasi merupakan aset vital bagi perguruan tinggi termasuk di Sekolah Tinggi Multi Media (STMM). Perkembangan teknologi informasi membawa manfaat besar, namun juga menghadirkan risiko terhadap keamanan informasi, termasuk ancaman terhadap kerahasiaan, integritas, dan ketersediaan data akademik, perkuliahan, penelitian, maupun layanan akademik lainnya.
Oleh karena itu, diperlukan pedoman manajemen risiko keamanan informasi untuk memastikan perlindungan informasi, serta mewujudkan lingkungan yang aman, terpercaya, dan mendukung keberlangsungan seluruh layanan akademik dan non akademik.

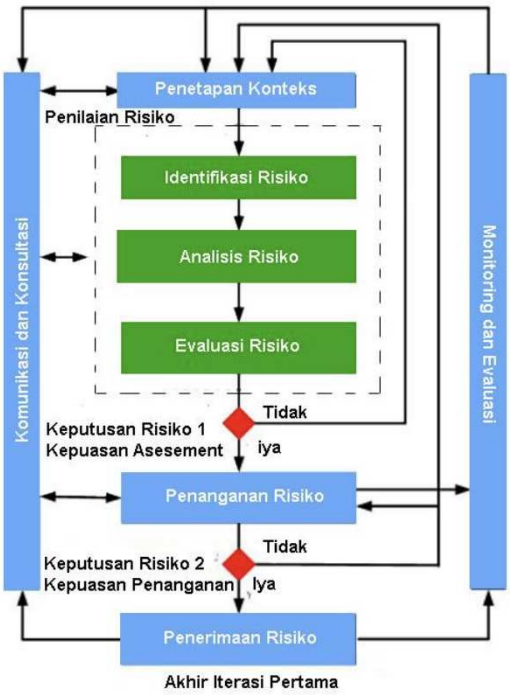
B. Maksud dan Tujuan

Dokumen ini bertujuan untuk memberikan panduan dalam mengidentifikasi, menganalisis, mengevaluasi, dan mengendalikan risiko keamanan informasi di lingkungan STMM, dengan tujuan untuk:

1. Menjamin keberlangsungan layanan informasi perguruan tinggi;
2. Melindungi aset informasi dari berbagai ancaman;
3. Meningkatkan kesadaran *civitas academica* terhadap pentingnya keamanan informasi;
4. Mewujudkan tata kelola keamanan informasi yang efektif dan akuntabel.

C. Proses Manajemen Risiko Keamanan Informasi

Secara garis besar, tahapan proses manajemen risiko dibagi menjadi 5 tahap yang meliputi komunikasi dan konsultasi, penetapan konteks, penanganan risiko, penerimaan risiko, serta monitoring dan evaluasi.
Berikut adalah diagram alur proses manajemen risiko berdasarkan ISO/IEC 27005:



Gambar 1: Alur Proses Manajemen Risiko

1. Komunikasi dan Konsultasi

Komunikasi dan konsultasi dilakukan terhadap para pemangku kepentingan dengan melibatkan unit dan tim kerja, maupun pihak eksternal. Komunikasi dan konsultasi sangat penting untuk dilakukan disetiap tahap proses manajemen risiko.

Komunikasi dan konsultasi dilakukan di sepanjang periode penerapan manajemen risiko, selaras dengan tahapan proses manajemen risiko dan berbagi kegiatan yang dilakukan dalam rangka penerapan manajemen risiko. Komunikasi dan konsultasi dilakukan dengan menggunakan beberapa mekanisme, diantaranya rapat berkala, rapat insidental, diskusi kelompok terarah, sosialisasi, dan media komunikasi lain yang disepakati di lingkungan STMM.

2. Penetapan Konteks

Dalam tahapan ini dilakukan penentuan ruang lingkup sistem informasi dan aset yang menjadi objek pengamanan, batasan, dan kriteria risiko yang relevan.

Langkah-langkah utama meliputi:

a. Menetapkan tujuan keamanan informasi STMM;
b. Mengidentifikasi aset informasi yang ada di STMM;
c. Menentukan peraturan, standar, dan kebijakan yang berlaku;
d. Menentukan toleransi risiko dan metode evaluasi risiko.

2.1 Identifikasi Risiko

Identifikasi risiko dilakukan dengan tujuan untuk menentukan sumber, penyebab, dan potensi dampak risiko yang dapat mempengaruhi keamanan informasi.

Terdapat beberapa tahapan yang bisa dilalui:

a. Memahami proses bisnis organisasi.
   Proses bisnis organisasi meliputi proses bisnis utama dan proses bisnis pendukung mengacu pada proses bisnis organisasi yang telah disahkan atau disetujui;
b. Mengidentifikasi kejadian risiko *(risk event)*
   Kejadian risiko dapat berupa kesalahan atau kegagalan yang mungkin terjadi pada tiap proses bisnis, pelaksanaan inisiatif strategis, atau faktor-faktor yang mempengaruhi pelaksanaan proses bisnis ataupun sasaran organisasi.
   Proses identifikasi risiko mencakup beberapa aspek sebagai berikut:
   - Identifikasi Aset – Menentukan aset informasi (data, perangkat keras, perangkat lunak, jaringan, SDM) yang bernilai bagi organisasi.
   - Identifikasi Ancaman – Menentukan potensi sumber gangguan, baik internal maupun eksternal (misalnya serangan siber, bencana, kesalahan manusia).
   - Identifikasi Kontrol yang Ada – Mengevaluasi pengendalian keamanan yang telah diterapkan.
   - Identifikasi Kerentanan – Mengidentifikasi kelemahan sistem atau proses yang dapat dimanfaatkan oleh ancaman.
   - Identifikasi Konsekuensi – Menilai dampak yang dapat terjadi jika risiko terealisasi, seperti kehilangan data, reputasi, atau gangguan operasional.
c. Mencari penyebab
   Berdasarkan risiko yang telah diidentifikasi, dilakukan identifikasi akar masalah yang menyebabkannya. Pemahaman mengenai akar masalah akan membantu menemukan tindakan yang dapat dilakukan untuk menangani risiko.
d. Menentukan dampak
   Dilakukan identifikasi dampak negatif yang mungkin terjadi berdasarkan risiko. Dampak merupakan akibat langsung yang timbul dan dirasakan setelah risiko terjadi. Apabila terdapat beberapa dampak langsung, ditetapkan satu dampak yang paling besar pengaruhnya terhadap pencapaian sasaran. Penentuan area dampak mengacu pada kriteria dampak.
e. Menentukan kategori risiko
   Berdasarkan risiko yang telah diidentifikasi, ditetapkan kategori risiko yang berlaku di STMM.
   Risiko dapat diklasifikasikan dalam beberapa bentuk sebagai berikut:

- Risiko Kepatuhan
  Risiko yang disebabkan karena pihak internal atau eksternal tidak mematuhi dan/atau tidak melaksanakan peraturan perundang-undangan, kebijakan, dan ketentuan lain yang berlaku.
- Risiko Hukum
  Risiko yang disebabkan oleh adanya tuntutan atau permasalahan hukum kepada organisasi.
- Risiko Kecurangan *(fraud)*
  Risiko penyalahgunaan akun oleh pihak internal maupun eksternal yang disebabkan oleh kecurangan yang disengaja sehingga menyebabkan kerugian.
- Risiko Reputasi
  Risiko yang disebabkan oleh menurunnya tingkat kepercayaan pemangku kepentingan eksternal yang bersumber dari persepsi negatif terhadap organisasi.
- Risiko Operasional
  Risiko yang disebabkan oleh ketidakcukupan dan/atau tidak berfungsinya proses internal, kesalahan manusia, dan kegagalan sistem serta adanya kejadian eksternal yang mengganggu kelancaran layanan.
- Risiko Keamanan Aset dan Informasi
  Risiko yang disebabkan kerusakan atau kehilangan aset informasi.
- Risiko Kebocoran dan Kehilangan Data
  Risiko di mana data penting diakses, digunakan, diubah, atau dimusnahkan oleh pihak yang tidak berwenang, atau hilang karena faktor internal maupun eksternal.
- Risiko Pengelolaan Informasi dan Data Pribadi
  Risiko yang mencakup potensi terjadinya insiden, pelanggaran hukum, atau gangguan operasional yang disebabkan oleh kegagalan organisasi dalam mengumpulkan, menyimpan, menggunakan, mengungkapkan, atau menghapus data pribadi dan informasi penting lainnya secara tepat, sah, dan aman.

Identifikasi risiko STMM tergambar dalam daftar risiko seperti yang terdapat pada Lampiran 2.

2.2 . Analisis Risiko

Analisis risiko bertujuan untuk mengukur tingkat risiko berdasarkan kemungkinan terjadinya ancaman dan besarnya dampak risiko terhadap aset informasi. Hasil analisis digunakan untuk mengkategorikan risiko menjadi sangat rendah, rendah, sedang, tinggi, atau sangat tinggi.

Penilaian risiko dilakukan dengan menggunakan dua parameter utama yaitu: tingkat kemungkinan *(likelihood)* dan tingkat dampak *(impact).*

a. Tingkat Kemungkinan

Tingkat kemungkinan dibagi menjadi 5 skala, seperti dalam tabel berikut:

Tabel 1. Kriteria Kemungkinan

Level Kemungkinan		**Kriteria Kemungkinan**
Skala	**Kategori**	**Probabilitas**
1	Sangat Rendah	Sangat jarang terjadi, <2 kali dalam 1 tahun
2	Rendah	Jarang terjadi, 2 s.d 5 kali dalam 1 tahun
3	Sedang	Terjadi 6 s.d 8 kali dalam 1 tahun
4	Tinggi	Terjadi 9 s.d 11 kali dalam 1 tahun
5	Sangat Tinggi	Terjadi =>12 kali dalam 1 tahun

b. Tingkat Dampak

Tingkat dampak dibagi menjadi 5 level sebagai berikut:

1) Sangat Rendah (Level 1)
   - Gangguan memiliki efek minimal pada layanan atau proses.
   - Tidak ada informasi sensitif yang terpengaruh.
   - Tidak menimbulkan kerugian finansial atau reputasi.
   - Operasional dapat tetap berjalan tanpa hambatan berarti.
   - Pemulihan sangat cepat dan tanpa memerlukan sumber daya tambahan.

2) Rendah (Level 2)
   - Gangguan menimbulkan dampak kecil pada proses kerja.
   - Informasi non-kritis mungkin terpengaruh namun tidak menimbulkan risiko besar.
   - Kerugian finansial sangat kecil atau dapat diabaikan.
   - Reputasi organisasi tidak terdampak atau hanya sangat minor.
   - Pemulihan dapat dilakukan dengan sedikit usaha dari tim terkait.

3) Sedang (Level 3)
   - Gangguan mulai memengaruhi beberapa layanan atau unit.
   - Beberapa data penting terpengaruh, tetapi masih dapat dipulihkan.
   - Menimbulkan kerugian finansial moderat.

- Reputasi organisasi berpotensi terkena dampak jika tidak ditangani.
- Membutuhkan koordinasi antarunit untuk pemulihan.

4) Tinggi (Level 4)
   - Gangguan menyebabkan layanan utama terganggu atau berhenti sementara.
   - Data sensitif atau penting berpotensi hilang, rusak, atau bocor.
   - Kerugian finansial signifikan.
   - Mempengaruhi kepercayaan pemangku kepentingan.
   - Pemulihan memerlukan sumber daya besar, waktu lama, dan prioritas tinggi.

5) Sangat Tinggi (Level 5)
   - Gangguan menyebabkan terhentinya operasi kritis atau layanan utama secara total.
   - Kebocoran/hilangnya data sangat sensitif (misalnya data pribadi, keuangan, strategis).
   - Dampak besar terhadap keberlangsungan institusi dan reputasi nasional.
   - Potensi sanksi hukum atau regulasi.
   - Pemulihan sangat sulit, memakan waktu lama, dan membutuhkan intervensi manajemen puncak.

Nilai atau besaran risiko diperoleh dengan mengalikan tingkat kemungkinan dan tingkat dampak. Besaran risiko dituangkan dalam matriks untuk menentukan level risiko. Level kemungkinan, level dampak, dan level risiko masing-masing menggunakan 5 skala tingkatan. Matriks analisis risiko disajikan dalam bentuk tabel sebagai berikut:

Tabel 2. Matriks Analisis Risiko

Matriks Analisis Risiko			Tingkat Dampak				
			1	2	3	4	5
			Sangat Rendah	Rendah	Sedang	Tinggi	Sangat Tinggi
Tingkat Kemungkinan	5	Sangat Tinggi	11	15	18	23	25
	4	Tinggi	6	12	16	19	24
	3	Sedang	4	8	14	17	22
	2	Rendah	2	7	10	13	21
	1	Sangat Rendah	1	3	5	9	20

Level risiko disajikan dalam bentuk tabel sebagai berikut:

Tabel 3. Level Risiko

Tingkatan	Level Risiko	Besaran Risiko	Warna
5	Sangat Tinggi	20-25	Merah
4	Tinggi	16-19	Orange
3	Sedang	11-15	Kuning
2	Rendah	6-10	Hijau
1	Sangat Rendah	1-5	Biru

2.3. Evaluasi Risiko

Evaluasi risiko dilakukan untuk menentukan prioritas penanganan risiko berdasarkan hasil analisis tingkat keparahan. Risiko dibandingkan dengan kriteria penerimaan risiko yang telah ditetapkan untuk menentukan tindakan selanjutnya.

Tabel 4. Prioritas Risiko

Tingkatan	Level	Prioritas Risiko	Besaran Risiko	Warna
5	Sangat Tinggi	1	25	
		2	24	
		3	23	
		4	22	
		5	21	
4	Tinggi	6	20	
		7	19	
		8	18	
		9	17	
		10	16	
3	Sedang	11	15	
		12	14	
		13	13	
		14	12	
		15	11	
2	Rendah	16	10	
		17	9	
		18	8	
		19	7	
		20	6	
1	Sangat Rendah	21	5	
		22	4	
		23	3	
		24	2	
		25	1	

Evaluasi risiko dilakukan melalui penyusunan prioritas risiko berdasarkan besaran risiko dengan ketentuan sebagai berikut:

a. Besaran risiko tertinggi mendapat prioritas paling tinggi;
b. Penentuan prioritas risiko dapat ditentukan setelah mengetahui besaran risikonya;
c. Apabila terdapat lebih dari satu risiko yang memiliki besaran risiko yang sama maka prioritas risiko ditentukan berdasarkan urutan area dampak dari yang tertinggi hingga terendah sesuai kriteria dampak;
d. Apabila masih terdapat lebih dari suatu risiko yang memiliki besaran dan area dampak yang sama maka prioritas risiko ditentukan berdasarkan urutan kategori risiko yang tertinggi hingga terendah sesuai dengan kategori risiko; dan
e. Apabila masih terdapat lebih dari satu risiko yang memiliki besaran, area dampak, dan kategori yang sama maka prioritas risiko ditentukan berdasarkan *judgement* pemilik risiko.

3. Penanganan Risiko

Penanganan risiko melibatkan pemilihan dan penerapan tindakan untuk mengurangi atau mengendalikan risiko hingga berada pada tingkat yang dapat diterima. Strategi yang dapat digunakan meliputi:

- Mitigasi - mengurangi kemungkinan atau dampak risiko.
- Transfer - mengalihkan risiko kepada pihak lain.
- Penghindaran - menghentikan aktivitas yang menimbulkan risiko.
- Penerimaan - menerima risiko apabila dampaknya kecil atau biaya mitigasinya lebih besar daripada manfaatnya.

Tindakan-tindakan pengendalian risiko dapat dikembangkan dari proses identifikasi dan evaluasi risiko berdasarkan matriks penilaian risiko. Selanjutnya tindakan pengendalian tersebut dapat diidentifikasi sebagai berikut:

1) Tidak Efektif : Pelaksanaan kontrol tidak berjalan baik dan tidak dimonitor sehingga tidak mempengaruhi tingkat risiko.
2) Kurang Efektif : Pelaksanaan kontrol tidak berjalan konsisten dan terjadi berulang kembali sehingga tidak sepenuhnya mampu mengurangi atau meminimalkan tingkat risiko.
3) Efektif : Penerapan kontrol sudah cukup baik dan konsisten sehingga dapat mengurangi / meminimalkan tingkat risiko.

4. Penerimaan Risiko

Tahap akhir dalam manajemen risiko adalah penerimaan risiko, yaitu proses peninjauan dan pengambilan keputusan secara formal untuk menerima risiko yang tersisa *(residual risk*) setelah dilakukan upaya penanganan. Keputusan ini didasarkan pada pertimbangan bahwa risiko tersebut berada dalam batas toleransi yang dapat diterima oleh STMM. Penerimaan risiko harus mendapat persetujuan dari pihak yang berwenang dan didokumentasikan secara resmi dalam daftar risiko *(risk register)* sebagai bukti akuntabilitas serta dasar untuk peninjauan dan perbaikan berkelanjutan dalam pengelolaan risiko.

5. Monitoring dan Evaluasi

Proses manajemen risiko harus terus dimonitor dan dievaluasi untuk memastikan bahwa proses pengamanan informasi masih sejalan dengan strategi dan sasaran organisasi. Proses monitoring dan evaluasi ini dilakukan secara berkala. Sehingga tujuan dari tahapan ini adalah meninjau efektivitas pengendalian risiko dan melakukan perbaikan berkelanjutan.

Setiap unit wajib mencatat hasil identifikasi, analisis, dan tindakan penanganan risiko dalam dokumen laporan. Laporan manajemen risiko disampaikan secara berkala kepada pimpinan STMM untuk dievaluasi dan ditindaklanjuti.

D. Penutup

Pedoman ini menjadi acuan bagi seluruh unit kerja di lingkungan Sekolah Tinggi Multi Media dalam melaksanakan manajemen risiko keamanan informasi. Diharapkan pedoman ini dapat meningkatkan kesadaran dan kesiapan seluruh *civitas academica* dalam menjaga keamanan informasi serta mendukung tata kelola perguruan tinggi yang baik.

Ditetapkan di Yogyakarta
Pada tanggal 17 November 2025

KETUA,

R.M. AGUNG HARIMURTI

No	Nama	Jabatan	Paraf
1.	RB Hendri K	Puket II	
2.	Candra S	Kanit TIK	
3.	Triawan S	Ketua SPI	

LAMPIRAN II
KEPUTUSAN KETUA SEKOLAH TINGGI MULTI MEDIA
NOMOR 355 TAHUN 2025
TENTANG
MANAJEMEN RISIKO KEAMANAN INFORMASI DI LINGKUNGAN SEKOLAH TINGGI MULTI MEDIA

Daftar Risiko Aset Informasi Sekolah Tinggi Multi Media

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Nilai Risiko	Pengendalian yang Ada	Rencana Mitigasi	Penanggung Jawab
1	Sistem Informasi Akademik	*Web defacement,* akses tidak sah	OS tidak *update*	Gangguan layanan, kebocoran data	Tinggi	Sertifikat SSL HTTPS, Manajemen Akses berbasis peran, Pemantauan Keamanan *Website* berkala	*Update OS, Update* perangkat lunak	Sistem: Unit TIK Data dan konten: Bagian Administrasi Akademik
2	Sistem Informasi Perpustakaan	*Web defacement,* akses tidak sah	OS tidak *update*	Gangguan layanan, kebocoran data	Tinggi	Sertifikat SSL HTTPS, Manajemen Akses berbasis peran, Pemantauan Keamanan *Website* berkala	*Update OS, Update* perangkat lunak	Sistem: Unit TIK Data dan konten: Unit Perpustakaan

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Nilai Risiko	Pengendalian yang Ada	Rencana Mitigasi	Penanggung Jawab
3	Sistem Informasi Tagihan Mahasiswa	*Web defacement,* akses tidak sah	OS tidak *update*	Gangguan layanan, kebocoran data	Tinggi	Sertifikat SSL HTTPS, Manajemen Akses berbasis peran, Pemantauan Keamanan *Website* berkala, VPN untuk interkoneksi ke kemenkeu	*Update OS, Update* perangkat lunak	Sistem: Unit TIK Data dan konten: Tim Keuangan
4	Sistem Informasi Penerimaan Mahasiswa Baru	*Web defacement,* akses tidak sah	OS tidak *update*	Gangguan layanan, kebocoran data	Tinggi	Sertifikat SSL HTTPS, Manajemen Akses berbasis peran, Pemantauan Keamanan *Website* berkala	*Update OS, Update* perangkat lunak	Sistem: Unit TIK Data dan konten: Bagian Administrasi Akademik
5	LMS *(e-learning)*	Kegagalan konfigurasi/ *setting* pada LMS	Versi moodle kurang *update*	Gangguan layanan, data tidak tersimpan	Sedang	HTTPS, akses *login OAuth*, manajemen akses	2FA	Unit TIK

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Nilai Risiko	Pengendalian yang Ada	Rencana Mitigasi	Penanggung Jawab
6	Data Mahasiswa	Data tidak ter-*backup*, akses ilegal	*Backup* data	Kehilangan data, kebocoran data sensitif	Sedang	Manajemen Akses berbasis peran, 2FA, penggantian *password* berkala	*Backup* data, enkripsi, file *sharing* berbasis akses	Tim Administrasi Akademik
7	*Open Journal System*	Data tidak ter-*backup*, akses ilegal	*Backup* data	Kehilangan data, kebocoran data sensitif	Sedang	Sertifikat SSL HTTPS, Manajemen Akses berbasis peran, Pemantauan Keamanan *Website* berkala	*Update* versi OJS, *update* OS	Sistem: Unit TIK Data dan konten: PPPM
8	*Website* dengan sub domain mmtc.ac.id	*Web defacement*, akses tidak sah	OS tidak *update*	Gangguan layanan, kebocoran data	Tinggi	Sertifikat SSL HTTPS, Manajemen Akses berbasis peran, Pemantauan Keamanan *Website* berkala	*Update OS, Update* perangkat lunak	Sistem: Unit TIK Data dan konten: Pemohon sub domain
9	Akun Google *workspace* STMM	Akun diretas, file dibagikan publik	Tanpa 2FA *Weak Password*	Kebocoran akun dan dokumen	Tinggi	HTTPS, manajemen akses berbasis peran, pemantauan aktivitas/login *unsecured*, antivirus	2FA	Unit TIK

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Nilai Risiko	Pengendalian yang Ada	Rencana Mitigasi	Penanggung Jawab
10	Infrastruktur Jaringan Kampus	Pemadaman listrik	Butuh waktu *up* genset	Layanan lumpuh sementara	Rendah	VLAN, *bandwidth control*, monitoring	*Bandwidth* control, VPN bagi Unit TIK	Unit TIK
11	CCTV	Akses ilegal, sabotase perangkat	*Backup* tidak tervalidasi	Data *backup* tidak tersimpan	Rendah	Akses terbatas, *Backup* minimal 30 hari, *Recorder* terpusat dan di lokasi gedung	*Backup* berkala	Unit TIK
12	Server	Kegagalan *hardware, overheating, malware*	*Patch* kurang *update*	Gangguan layanan, kebocoran data	Sedang	CCTV, kunci pintu biometrik, UPS, *backup* data rutin	Akses berbasis peran, log audit, APAR CO2/*liquid gas*	Unit TIK

Ditetapkan di Yogyakarta
Pada tanggal 17 November 2025
KETUA,

R.M. AGUNG HARIMURTI

No	Nama	Jabatan	Paraf
1.	RB Hendri K	Puket II	
2.	Candra S	Kanit TIK	
3.	Triawan S	Ketua SPI	