





PT INFOMEDIA NUSANTARA

**Prosedur
Manajemen Insiden Keamanan Informasi**

No. Dokumen	IN.PRO-20
Versi	1.0
Klasifikasi	Terbatas
Tanggal Efektif	08 September 2021
Tanggal Peninjauan	-
Jenis Dokumentasi	Pedoman / Prosedur
Pemilik Dokumen	Koordinator Pengelolaan Insiden

PERSETUJUAN:

DISUSUN:	MENGETAHUI:	DISETUJUI:
		
<u>Firdiansyah</u> Pengendali Dokumen	<u>Samudra Prasetio</u> Wakil Manajemen	<u>Agus Winarno</u> Manajemen Puncak


	Prosedur Manajemen Insiden	PT Infomedia Nusantara	
		No. Dokumen	IN.PRO-20
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	2

RIWAYAT PERUBAHAN

Versi	Penyusun / Pelaksana Revisi	Tanggal Revisi	Keterangan Perubahan	Bab	Hal
1.0	Pengendali Dokumen	08 September 2021	Versi pertama	-	-
			CC TELKOM		

**CONTROLLED
DOCUMENT**

MALANG


	Prosedur Manajemen Insiden	PT Infomedia Nusantara	
		No. Dokumen	IN.PRO-20
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	3

DAFTAR ISI

Hal.

RIWAYAT PERUBAHAN	2
DAFTAR ISI	3
1. TUJUAN.....	1
2. RUANG LINGKUP	1
3. REFERENSI	1
4. DEFINISI.....	1
5. KEBIJAKAN UMUM	1
5.1. Pelaporan Kejadian, Kelemahan, dan Insiden Keamanan Informasi	1
5.2. Penanganan Kejadian Kelemahan dan Insiden Keamanan Informasi	3
5.3. Evaluasi Pembelajaran Kejadian Kelemahan dan Insiden Keamanan Informasi	3
5.4. Pengumpulan Bukti	4
6. PENGKAJIAN DOKUMEN	4
7. LAMPIRAN.....	4

MALANG

	<p style="text-align: center;">Prosedur Manajemen Insiden</p>	PT Infomedia Nusantara	
		No. Dokumen	IN.PRO-20
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	1

1. TUJUAN

Kebijakan dan prosedur ini bertujuan untuk mengelola pelaporan kejadian kelemahan dan insiden terkait keamanan informasi agar dilakukan melalui cara yang tepat dan cepat sehingga tindakan perbaikan dilakukan dengan tepat dan cepat serta memastikan pendekatan yang konsisten dan efektif dalam pengelolaan kelemahan dan kejadian insiden keamanan informasi.

2. RUANG LINGKUP

Kebijakan dan Prosedur ini berlaku untuk proses pelaporan dan penanganan kelemahan dan kejadian insiden serta evaluasi dan pembelajaran dari kejadian, kelemahan dan insiden keamanan informasi dan pengumpulan bukti pendukung bagi tindakan legal dalam ruang lingkup SMKI di PT Infomedia Nusantara.

3. REFERENSI

ISO 27001:2013; Annex A.16 - Pengelolaan Insiden Keamanan Informasi


4. DEFINISI

- **Insiden (SMKI)**
Merupakan kejadian keamanan informasi merupakan hal-hal yang dapat mengindikasikan adanya potensi insiden keamanan informasi yang dapat menyebabkan berkurangnya atau hilangnya aspek kerahasiaan, integritas, dan ketersediaan dari informasi.
- **Kelemahan (Potensi Ketidaksesuaian)**
Merupakan kejadian atau hal-hal yang berpotensi dapat dieksploitasi oleh pihak yang tidak bertanggung jawab sehingga menimbulkan gangguan dan/atau kegagalan suatu proses atau sistem serta pelanggaran terhadap ketentuan prasyarat standar yang telah ditetapkan.

5. KEBIJAKAN UMUM

5.1. Pelaporan Kejadian, Kelemahan, dan Insiden Keamanan Informasi

1. Ketika terjadi sebuah kejadian / kelemahan / insiden keamanan informasi, pegawai, penyedia, dan pengguna pihak ketiga harus sesegera mungkin mengambil bukti (*evidence*) atas kejadian / kelemahan / insiden keamanan yang terjadi untuk kemudian dilaporkan.
2. Pegawai dan/atau pihak ketiga melaporkan insiden atau kelemahan kepada Koordinator Pengelola Insiden dengan cara:
 - a) Melalui formulir laporan insiden, apabila terjadi insiden keamanan informasi yang dapat ditangani oleh pihak internal PT Infomedia Nusantara.

	Prosedur Manajemen Insiden	PT Infomedia Nusantara	
		No. Dokumen	IN.PRO-20
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	2

3. Pegawai, penyedia, dan pengguna pihak ketiga harus diberikan edukasi mengenai tanggung jawab untuk melaporkan kelemahan / insiden keamanan informasi secepat mungkin.
4. Pelaporan kejadian / kelemahan / insiden keamanan informasi dilakukan / ditujukan untuk dicatat oleh Koordinator Pengelola Insiden dan dapat dieskalasi kembali.
5. Contoh insiden keamanan informasi dapat mencakup namun tidak terbatas pada hal-hal sebagai berikut.
 - a) Kehilangan aset informasi dan TI seperti *notebook*, *harddisk* atau dokumen milik PT Infomedia Nusantara.
 - b) Ketidakpatuhan pada kebijakan dan prosedur terkait keamanan informasi.
 - c) Pelanggaran terkait keamanan fisik.
 - d) Kegagalan perangkat lunak, perangkat keras, atau sarana pendukung seperti Bugs, jaringan komunikasi, listrik, atau AC.
 - e) Kesalahan manusia (human error).
 - f) Perubahan sistem yang tidak terotorisasi.
6. Keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut.


Klasifikasi	Deskripsi
Mayor	Apabila insiden tersebut menyebabkan terhentinya proses pekerjaan utama di PT Infomedia Nusantara
Minor	Apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses pekerjaan di PT Infomedia Nusantara

7. Insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut.

Klasifikasi	Deskripsi
<i>Emergency</i>	Apabila insiden tersebut terjadi harus segera diselesaikan kurang dalam 1 hari (24 jam).
Normal	Apabila insiden tersebut terjadi harus diselesaikan kurang dari 4 hari (96 jam)

8. Insiden keamanan informasi yang bersifat mayor dan *emergency* harus dilaporkan kepada Manajemen Puncak PT Infomedia Nusantara.
9. Urutan prioritas penanganan kejadian / kelemahan / insiden keamanan informasi adalah sebagai berikut.

Urutan Prioritas	Klasifikasi / Kategori Insiden
1	Insiden <i>Emergency</i> - <i>Major</i>
2	Insiden <i>Emergency</i> - <i>Minor</i>
3	Insiden <i>Normal</i> - <i>Major</i>
4	Insiden <i>Normal</i> - <i>Minor</i>

	<p style="text-align: center;">Prosedur Manajemen Insiden</p>	PT Infomedia Nusantara	
		No. Dokumen	IN.PRO-20
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	3

5

Kejadian dan Kelemahan keamanan informasi


10. Kejadian dan kelemahan yang belum menjadi insiden keamanan informasi perlu mendapat evaluasi yang lebih mendalam serta dapat dikonsultasikan kepada pihak yang relevan dengan kejadian dan kelemahan tersebut.

5.2. Penanganan Kejadian Kelemahan dan Insiden Keamanan Informasi

1. Setiap kejadian / kelemahan / insiden keamanan informasi harus dianalisis dan dievaluasi secara seksama agar dapat ditentukan langkah tindak lanjut penanganan yang tepat dan cepat.
2. Penanganan dari kejadian / kelemahan / insiden keamanan informasi harus dilakukan dengan prinsip sebagai berikut.
 - a. Memulihkan kondisi sedemikian rupa sehingga aktivitas pekerjaan di PT Infomedia Nusantara dapat segera dilaksanakan kembali.
 - b. Meminimalisir dampak dari kejadian / kelemahan / insiden keamanan informasi.
3. Setiap laporan kejadian / kelemahan / insiden keamanan informasi beserta penanganannya harus terdokumentasikan dengan baik.

5.3. Evaluasi Pembelajaran Kejadian Kelemahan dan Insiden Keamanan Informasi

1. Evaluasi dari kejadian dan kelemahan keamanan informasi dilakukan dengan cara mengidentifikasi kejadian dan kelemahan yang terjadi beserta penyebab utamanya (*root cause*) untuk mencegah terjadinya insiden yang dapat terjadi.
2. Evaluasi insiden keamanan informasi dilakukan dengan cara mengidentifikasi insiden yang berulang atau insiden dengan dampak besar beserta penyebab utamanya (*root cause*) untuk dapat diambil tindakan untuk mencegah terulangnya kembali insiden tersebut.
3. Setelah kejadian dan kelemahan telah teridentifikasi atau insiden keamanan informasi telah diselesaikan/ditutup, perlu dilakukan kegiatan peninjauan yang berikut.
 - a) Mengidentifikasi penyebab utama (*root cause*) dari kejadian, kelemahan dan insiden keamanan informasi.
 - b) Mengidentifikasi pelajaran yang diperoleh (pengalaman) dari insiden keamanan informasi.
 - c) Mengidentifikasi perbaikan terhadap pelaksanaan perlindungan keamanan informasi, sebagai hasil dari pelajaran yang diperoleh, baik dari satu atau lebih kejadian, kelemahan dan insiden keamanan informasi.
 - d) Mengidentifikasi perbaikan terhadap skema pengelolaan insiden keamanan informasi secara keseluruhan, sebagai hasil pelajaran yang diperoleh dari peninjauan jaminan mutu terhadap sebuah pendekatan (sebagai contoh, dari tinjauan atas keefektifan proses, prosedur, formulir pelaporan dan/atau struktur organisasi).
4. Peninjauan dilanjutkan dengan perbaikan yang meliputi aktivitas sebagai berikut.

	<p style="text-align: center;">Prosedur Manajemen Insiden</p>	PT Infomedia Nusantara	
		No. Dokumen	IN.PRO-20
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	4

- a. Perbaikan atau penyesuaian analisa risiko keamanan informasi organisasi yang telah ada.
- b. Peningkatan skema dari pengelolaan insiden keamanan informasi dan dokumentasinya.
- c. Perbaikan keamanan, yang meliputi implementasi dari perlindungan keamanan informasi baru dan/atau yang dimutakhirkan.

5.4. Pengumpulan Bukti

1. Pengumpulan bukti atas pelaporan dan penanganan insiden harus dilakukan oleh Koordinator Pengelolaan Insiden secara memadai dan efektif. Hal ini merupakan pertimbangan yang penting jika terjadi tuntutan hukum di kemudian hari dan tindakan sabotase yang dilakukan secara sengaja atau audit forensik terhadap kelemahan sistem ataupun infrastruktur yang terjadi.
2. Bukti atas pelaporan dan penanganan insiden harus dijaga dari aspek integritas dan ketersediaannya saat dibutuhkan.
3. Masa retensi penyimpanan bukti atas pelaporan dan insiden harus ditetapkan di dalam Formulir Aset Informasi.
4. Jika informasi telah melewati masa retensinya dapat dilakukan penyalinan bukti atas pelaporan dan insiden ke dalam bentuk *softcopy* atau digital untuk menjaga dari kerusakan dan kehilangan yang mungkin dapat terjadi.
5. Pelanggaran atas pengumpulan dan pelestarian bukti pelaporan insiden dapat diberi sanksi sesuai dengan peraturan perusahaan yang berlaku.

6. PENGKAJIAN DOKUMEN

Dokumen ini dikelola oleh Koordinator Standar, Kepatuhan dan Dokumen. Setiap masukan perubahan terhadap prosedur ini harus diajukan kepada Koordinator Standar, Kepatuhan dan Dokumen. Perubahannya disetujui oleh Manajemen Puncak sesuai ketentuan yang berlaku di PT Infomedia Nusantara.

Dokumen ini harus ditinjau ulang secara berkala oleh Koordinator Standar, Kepatuhan dan Dokumen paling sedikit 1 (satu) kali dalam setahun untuk memastikan kesesuaiannya dengan kondisi organisasi.

7. LAMPIRAN

Laporan Insiden