
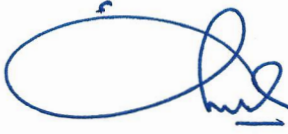




**PT INFOMEDIA NUSANTARA**

# **Pedoman Kebijakan Keamanan Informasi**

No. Dokumen	IN.PRO-02
Versi	1.0
Klasifikasi	Terbatas
Tanggal Efektif	08 September 2021
Tanggal Peninjauan	-
Jenis Dokumentasi	Pedoman / Prosedur
Pemilik Dokumen	Koordinator Pengendali Dokumen


**PERSETUJUAN:**

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

	<b>Pedoman Kebijakan Keamanan Informasi</b>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	1


## RIWAYAT PERUBAHAN

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

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	2

## DAFTAR ISI

	Hal.
RIWAYAT PERUBAHAN	i
DAFTAR ISI	ii
1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan	1
2. RUANG LINGKUP DOKUMEN	1
3. REFERENSI	2
SNI ISO/IEC 27002:2013	2
4. DEFINISI	2
5. KEBIJAKAN	4
5.1 Keamanan Informasi	4
5.2 Pengorganisasian Keamanan Informasi	4
5.3 Keamanan Personil	4
5.4 Keamanan Fisik dan Lingkungan	5
5.5 Penanganan Informasi	5
5.6 Penggunaan <i>Removable Media</i>	6
5.8 Pengelolaan Pihak Ketiga	7
5.9 Penggunaan Email dan Internet	7
5.10 Pengendalian Akses	8
5.11 Pengelolaan Password Aset Sistem dan Infrastruktur	8
5.12 Penggunaan Kriptografi	9
5.13 Pengelolaan Kunci Kriptografi	9
5.14 Pemeliharaan dan Operasional Sistem Informasi	10
5.15 Pengembangan dan Pemeliharaan Sistem Informasi	10
5.16 Manajemen Insiden	11
5.17 Kontinjensi dan Pemulihan Bencana	12
5.18 Kepatuhan	12
5.19 <i>Clear Desk</i> dan <i>Clear Screen</i>	12
5.20 Teleworking	13
5.21 Perangkat Bergerak ( <i>Mobile Device</i> )	14
6. PENGKAJIAN DOKUMEN	14
7. LAMPIRAN	14

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	3

## 1. PENDAHULUAN

### 1.1 Latar Belakang

Keamanan informasi menjadi hal yang sangat penting bagi PT Infomedia Nusantara dalam rangka memberikan layanan *Customer Relationship Management* dan Layanan *Shared Service Operations*. Penerapan keamanan informasi bertujuan untuk menjamin keberlangsungan ketersediaan informasi dari risiko yang mungkin terjadi yang dapat menyebabkan pengelolaan proses menjadi terganggu. Untuk itu, PT Infomedia Nusantara mempunyai tanggung jawab dalam mengelola informasi agar terhindar dari risiko kerusakan, kehilangan atau terungkapnya informasi ke pihak luar.


Proses perlindungan terhadap informasi tersebut harus dikelola dengan baik sehingga informasi yang dihasilkan dapat terjaga kerahasiaannya, keakuratan nya, dan ketersediaan secara efektif. Semakin banyak informasi Organisasi yang disimpan dan dikelola, maka semakin besar pula risiko terjadinya kerusakan, kehilangan atau terungkapnya informasi ke pihak luar yang tidak diinginkan. Proses perlindungan terhadap informasi tersebut harus dikelola dengan baik sehingga informasi yang dihasilkan dapat terjaga kerahasiaannya (*confidentiality*), keakuratan nya (*integrity*), dan ketersediaan (*availability*) secara efektif.

### 1.2 Sasaran

Sejalan dengan pentingnya informasi di layanan *Customer Relationship Management* dan Layanan *Shared Service Operations*, maka sasaran utama dari kebijakan keamanan informasi adalah memberikan arahan mengenai proses-proses keamanan informasi terkait dengan perlindungan terhadap aset teknologi informasi yang digunakan. Keamanan informasi dapat dicapai dengan penerapan secara menyeluruh dan konsisten terhadap kontrol keamanan informasi yang tertuang dalam kebijakan ini. Penggunaan dan pengelolaan informasi melatarbelakangi disusunnya kebijakan keamanan informasi yang mengacu pada standar internasional sistem manajemen keamanan informasi sebagai panduan dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan PT Infomedia Nusantara khususnya Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* di PT Infomedia Nusantara.

### 1.3 Tujuan

Kontrol keamanan informasi yang diterapkan pada lingkup PT Infomedia Nusantara bertujuan untuk:

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	4


- Menjamin kesinambungan layanan yang diberikan dengan cara menghindari atau setidaknya meminimalkan risiko bencana dan menghindari terjadinya pelanggaran-pelanggaran kaidah pengamanan serta mengurangi berbagai dampak kerugian yang potensial.
- Memenuhi persyaratan regulasi yang ditetapkan agar sesuai dengan peraturan regulasi khususnya di bidang *Business Process Outsourcing* di PT Infomedia Nusantara.
- Sebagai persyaratan kelengkapan sistem, tata kerja dan tata kelola layanan *Customer Relationship Management* dan Layanan *Shared Service Operation*.

## 2. RUANG LINGKUP

Ruang Lingkup Pedoman Sistem Manajemen Keamanan Informasi (SMKI) mencakup Ruang Lingkup yang ditetapkan dalam Surat Keputusan ini meliputi Sistem Manajemen Keamanan Informasi pada Layanan Customer Relationship Management dan Layanan Shared Service Operations serta Operasional Sistem Informasi, Aktivitas Dukungan Infrastruktur, dan Aplikasi HelpDesk terkait yang ada di PT Infomedia Nusantara.

## 3. REFERENSI

SNI ISO/IEC 27001:2013; Annex 9 – Access control  
 SNI ISO/IEC 27001:2013; Annex 8.2 – Information classification  
 SNI ISO/IEC 27001:2013; Annex 11 – Physical and environmental security  
 SNI ISO/IEC 27001:2013; Annex 8.1.3 – Acceptable use of assets  
 SNI ISO/IEC 27001:2013; Annex 11.2.9 – Clear desk and clear screen policy  
 SNI ISO/IEC 27001:2013; Annex 13.2.1–Security of network service  
 SNI ISO/IEC 27001:2013; Annex 6.2 – Mobile device and teleworking  
 SNI ISO/IEC 27001:2013; Annex 12.6.2 – Restrictions on software installation  
 SNI ISO/IEC 27001:2013; Annex 12.3 – Backup  
 SNI ISO/IEC 27001:2013; Annex 13.2 – Information transfer  
 SNI ISO/IEC 27001:2013; Annex 12.2 – Protection from malware  
 SNI ISO/IEC 27001:2013; Annex 12.6.1 – Management of technical vulnerabilities  
 SNI ISO/IEC 27001:2013; Annex 10 – Cryptography  
 SNI ISO/IEC 27001:2013; Annex 13 – Communication security  
 SNI ISO/IEC 27001:2013; Annex 18.1.4 – Privacy and protection of personally identifiable information  
 SNI ISO/IEC 27001:2013; Annex 15 – Supplier relationships

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	5

## 4. KEBIJAKAN KEAMANAN INFORMASI

### 4.1 Arahan Manajemen Untuk Keamanan Informasi

Kebijakan Keamanan informasi bertujuan untuk melindungi aset Organisasi yang dikelola dan digunakan agar terhindar dari berbagai ancaman internal maupun eksternal yang meliputi keamanan data, perangkat teknologi, infrastruktur dan sistem, seluruh aktivitas serta proses yang terkait dengan penyediaan informasi.

#### 4.1.1 Kebijakan Keamanan Informasi

Aturan Kebijakan:

- (1) Dokumen kebijakan keamanan informasi harus disetujui oleh Manajemen Puncak untuk penerapan di Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* di PT Infomedia Nusantara.
- (2) Dokumen Kebijakan Keamanan Informasi ini harus disosialisasikan kepada seluruh personil di PT Infomedia Nusantara.

#### 4.1.2 Peninjauan (*Review*) Kebijakan Keamanan Informasi

Aturan Kebijakan:

- (1) Dokumen kebijakan keamanan informasi harus dievaluasi setidaknya 1 kali dalam 1 tahun untuk menjaga kesesuaian efektifitas penerapannya.
- (2) Apabila dari hasil peninjauan terdapat perubahan maka harus dilakukan pengkinian terhadap dokumen kebijakan tersebut.


### 4.2 Mobile Computing dan Teleworking

Proses ini bertujuan untuk memastikan keamanan informasi saat bekerja menggunakan perangkat *mobile computing* dan aktivitas *teleworking*.

#### 4.2.1 Kebijakan perangkat *mobile*

Aturan Kebijakan:

- (1) Pengguna fasilitas *Notebook* harus menjaga keamanan dari perangkat dan informasi yang disimpan pada perangkat pada saat digunakan diluar area organisasi.
- (2) Penggunaan fasilitas *Notebook* di luar area PT Infomedia Nusantara harus dilengkapi dengan kontrol keamanan fisik untuk mencegah terjadinya pencurian/kehilangan perangkat.
- (3) Fasilitas *Notebook* milik PT Infomedia Nusantara tidak boleh ditinggalkan

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	6

tanpa pengawasan atau tanpa pengamanan pada saat digunakan diluar area PT Infomedia Nusantara.

- (4) Penggunaan fasilitas *Notebook* milik PT Infomedia Nusantara yang menyimpan informasi sensitif pada area publik, seperti restoran, stasiun, atau bandara harus sangat dibatasi.
- (5) Penggunaan fasilitas Wifi publik untuk mengirim informasi sensitif milik PT Infomedia Nusantara harus sangat dibatasi.

#### 4.2.2 Teleworking


Aturan Kebijakan:

- (1) Aktivitas *teleworking* didefinisikan sebagai aktivitas yang memungkinkan personil PT Infomedia Nusantara untuk bekerja secara *remote* dari sebuah lokasi tetap yang telah ditentukan, seperti rumah atau area kerja lain, diluar jaringan komunikasi PT Infomedia Nusantara.
- (2) Kegiatan *teleworking* dilaksanakan untuk keperluan kedinasan dan juga situasi yang *force majeure* (pandemi).
- (3) Personil yang akan melaksanakan kegiatan *teleworking* perlu memperhatikan lokasi tempat bekerja, antara lain sebagai berikut:
  - a. Menghindari bekerja di tempat umum yang terbuka,
  - b. Memperhatikan keamanan fisik sekitar lokasi tempat *teleworking* dilakukan.
- (4) Setiap jaringan lokal *teleworking* yang dipersiapkan harus memperhatikan faktor keamanan jaringan.

#### 4.3 Penggunaan Aset Yang Diterima

Aturan Kebijakan:


1. Aset informasi dan pengolahan informasi milik PT Infomedia Nusantara hanya boleh digunakan untuk kebutuhan pekerjaan PT Infomedia Nusantara.
2. Penggunaan perangkat pribadi untuk mengakses informasi dan jaringan komunikasi pada PT Infomedia Nusantara Harus melalui persetujuan Pimpinan terkait di Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations*
3. Pada saat jam kerja, penggunaan jaringan komunikasi dan layanan jaringan, seperti fasilitas internet serta *email*, milik PT Infomedia Nusantara hanya untuk kebutuhan pekerjaan.
4. Penggunaan fasilitas internet pada PT Infomedia Nusantara untuk melakukan akses ke situs-situs yang mengandung materi pornografi, kekerasan, materi yang dapat

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	7

mengundang kebencian terkait dengan suku, agama dan ras serta materi bajakan yang melanggar hak atas kekayaan intelektual, sangat dilarang.

5. Penggunaan modem data pada komputer milik PT Infomedia Nusantara dilarang dilakukan pada saat komputer tersebut terhubung ke jaringan komunikasi PT Infomedia Nusantara.
6. Menjaga kerahasiaan aset informasi dan/atau informasi yang ada di dalam suatu aset.
7. Tidak menggunakan aset untuk hal-hal yang bertentangan dengan etika, hukum dan merugikan Organisasi.
8. Pengguna akun bertanggung jawab atas keamanan data dan informasi yang berada/disimpan di dalam akunnya.
9. Pengguna akun tidak diperbolehkan untuk memberikan akses akunnya kepada orang lain, termasuk kepada atasan, bawahan, keluarga, dan/atau teman. Apabila suatu keadaan memerlukan untuk memberikan akses akun kepada orang lain, maka hal ini (atau keadaan yang mengharuskan untuk melakukan hal ini) harus mendapatkan persetujuan dari minimal manajemen setingkat Manager.
10. Password untuk akun *level* sistem dan akun *level* user harus dipelihara sesuai dengan kebijakan keamanan informasi mengenai *password*.
11. Ketika ditinggalkan, segala *mobile/portable device* seperti laptop, komputer tablet, dan *smartphone* yang digunakan untuk memproses informasi milik Organisasi (walaupun *device* tersebut adalah milik pribadi) harus dalam keadaan terkunci misalnya menggunakan kabel (sling) pengunci laptop atau disimpan di dalam laci/lemari yang terkunci.
12. Semua PC, komputer tablet, laptop, dan *smartphone* (termasuk perangkat pribadi) yang digunakan untuk memproses informasi milik Organisasi harus terlindungi dengan *password*.
13. *Screen lock (screen saver)* yang terproteksi oleh *password* harus secara otomatis aktif untuk semua PC, komputer tablet, laptop, *smartphone* (termasuk perangkat pribadi) yang digunakan untuk memproses informasi milik Organisasi, dalam waktu maksimum 10 menit perangkat tersebut dalam keadaan *idle*.
14. Ketika meninggalkan PC, komputer tablet, laptop, *smartphone* (termasuk perangkat pribadi) yang digunakan untuk memproses informasi, walaupun hanya sebentar, pastikan dalam keadaan *screen locked* yang terproteksi *password*.
15. Dilarang untuk melakukan instalasi / uninstallasi / reinstalasi aplikasi, fitur, ekstensi sistem operasi tanpa seizin administrator yang berwenang.
16. Apabila terjadi kehilangan/kerusakan terhadap aset komputasi yang digunakan untuk memproses informasi Organisasi (walaupun aset tersebut adalah milik pribadi) harus



	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	8

dilaporkan melalui mekanisme penanganan insiden.

#### 4.4 Klasifikasi Informasi

Untuk menjaga dan menjamin keamanan informasi, klasifikasi terhadap informasi perlu dilakukan dengan mempertimbangkan kebutuhan, prioritas, sensitivitas, dan kritikalitas dalam proses bisnis Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* dikelola PT Infomedia Nusantara.

##### 4.4.1 Klasifikasi Informasi


Aturan Kebijakan:

1. Klasifikasi jenis aset informasi di Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* dikelola PT Infomedia Nusantara disesuaikan dengan kebutuhan dan dampak bisnis. Klasifikasi tersebut meliputi:
  - Informasi Rahasia, yaitu informasi yang sangat sensitif dan hanya dapat diakses oleh individu / pihak tertentu.
  - Informasi Terbatas, yaitu data yang hanya dapat diakses secara internal dalam lingkungan PT Infomedia Nusantara.
  - Informasi Publik, yaitu informasi yang dapat disebarluaskan ke publik.
2. Setiap Pimpinan terkait di PT Infomedia Nusantara dapat mengklasifikasikan informasi yang dianggap perlu sebagai informasi rahasia, di luar ketentuan perundang-undangan yang berlaku untuk mencegah gangguan terhadap proses bisnis organisasi.
3. Perlindungan terhadap aset informasi harus dilakukan secara memadai sesuai dengan klasifikasinya.
4. Tingkat perlindungan aset informasi dilakukan sesuai dengan aturan penanganan informasi yang diterapkan di Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* dikelola PT Infomedia Nusantara.

##### 4.4.2 Pelabelan dan Penanganan Informasi

Aturan Kebijakan:

1. Informasi Harus diberi label/kode untuk memastikan penanganan informasi tersebut sesuai dengan tingkat klasifikasinya.
2. Pelabelan informasi dapat dilakukan melalui:
  - a. Pelabelan secara fisik pada dokumen *hardcopy*;
  - b. Pemberian *watermark* pada dokumen *softcopy*;

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	9

- c. Pemberian klasifikasi informasi pada *metadata* dari informasi *softcopy*.
3. Penanganan informasi harus dilakukan secara aman pada seluruh siklus hidup informasi yang mencakup proses pemrosesan, penyimpanan, distribusi, dan pemusnahan informasi.
4. Penanganan informasi perlu disesuaikan dengan klasifikasi dari informasi tersebut.
5. Laporan yang dicetak (Dokumen)
 


Bila memungkinkan, hasil cetakan dari informasi diberikan penanda yang menyatakan klasifikasi keamanan dari informasi dokumen sebagai *watermark*. *Watermark* tersebut haruslah terlihat jelas pada setiap halaman dokumen. Berikut metode yang dapat digunakan:

  - a. Klasifikasi akan ditampilkan secara jelas di halaman depan dan di *footer* sebelah kiri setiap halaman berikutnya;
  - b. Pra-cetak kertas menunjukkan klasifikasi keamanan yang akan digunakan; dan
  - c. Penggunaan cap digunakan untuk menandai setiap halaman dengan klasifikasi keamanan.
6. *Screen Displays*

Sistem komputer harus mengklasifikasi pengguna yang berwenang untuk dapat mengakses informasi termasuk peringatan pada saat akan *login*. Jika memungkinkan, pengguna akan diberikan peringatan apabila pengguna akan masuk kedalam sistem atau area yang bukan merupakan haknya. Peringatan lebih lanjut juga harus ditampilkan pada saat memasuki pilihan untuk mencetak atau menyimpan data dari sistem.
7. Media Rekaman
 

Kontrol yang ketat ditempatkan pada penggunaan *removable media* seperti CD, DVD, kaset, *hard drive* eksternal dan memori stick USB dalam organisasi. Dimana hal tersebut sah digunakan untuk menyimpan data rahasia mereka akan diberi label eksternal dengan klasifikasi keamanan dari data yang paling sensitif pada media, bersama-sama dengan tanggal pembuatan.
8. Surat Elektronik (*E-Mail*)
 

Informasi rahasia yang dikirim melalui surat elektronik harus mencakup tingkat klasifikasi jika dikirim ke eksternal, pernyataan kontrol yang harus ditempatkan informasi oleh penerima email. Informasi yang terkandung dalam lampiran, juga harus menyatakan klasifikasi jelas pada *header* dari jenis dokumen, *spreadsheet*, atau *file* lainnya.
9. *File Transfer*

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	10

Prosedur untuk mendapatkan informasi rahasia dikirim melalui transfer *file* harus menyertakan langkah di mana penerima jelas informasi dari tingkat klasifikasi informasi yang sedang dikirim, sebelum dikirim.

#### 4.5 Penanganan Aset

Aturan Kebijakan:

1. Penanganan terhadap aset harus sesuai dengan klasifikasi dari aset informasi yang disimpan dan/atau diproses oleh aset tersebut untuk memastikan keamanan dari aset informasi.
2. Untuk masing-masing tingkat klasifikasi keamanan satu set kontrol harus memastikan bahwa aset informasi yang terlibat secara tepat dilindungi setiap saat. Bagian berikut menetapkan komponen prosedural utama dari kontrol yang telah ada.

##### i) Publik

##### a) Proses Pengamanan

Secara umum tidak ada kontrol khusus yang harus ditempatkan pada pengolahan informasi tersebut, namun harus diingat bahwa barang-barang seperti alat tulis dan setara elektronik mereka tidak harus dibuat tersedia secara bebas.

##### b) Penyimpanan

Informasi dapat disimpan di daerah aman diakses oleh publik. Namun beberapa kontrol harus ditempatkan pada sejumlah besar informasi tersebut seperti leaflet yang masih bisa dikenakan terhadap pencurian atau penyalahgunaan.

##### c) Transmisi

Secara umum, informasi publik dapat dikirim melalui koneksi dan tidak terenkripsi atau didistribusikan secara bebas dalam bentuk *hard copy*.

##### d) Deklasifikasi


Informasi publik tidak akan dikenakan deklasifikasi karena sudah pada tingkat terendah.

##### e) Pemusnahan

Informasi yang termasuk dalam klasifikasi umum dapat dibuang melalui rute limbah normal tanpa perlu untuk kontrol seperti merobek-robek. Bila memungkinkan, barang-barang harus didaur ulang.

##### f) Proses pendistribusian Informasi

Aset informasi publik akan bebas didistribusikan di antara personel PT Infomedia Nusantara, pelanggan, dan anggota masyarakat di mana diperlukan.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	11

g) *Login* Keamanan

Pada umumnya tidak perlu *login* insiden keamanan yang berkaitan dengan item klasifikasi umum kecuali pada kegiatan kriminal seperti pencurian dokumen dalam skala besar.

ii) **Terbatas**

a) Proses Pengamanan

Informasi pada tingkat klasifikasi akan dikenakan untuk mengakses kontrol yang melibatkan baik keamanan fisik atau *log-on* penggunaan resmi atau keduanya. Akses untuk umum tidak boleh diberikan di tempat umum dan output seperti cetakan harus ke daerah-daerah di mana akses publik dicegah.

b) Penyimpanan

Informasi klasifikasi ini dapat disimpan pada media elektronik seperti kaset, DVD, dan CD. Media ini harus disimpan di ruang terkunci dan di daerah di mana tidak ada akses publik.

c) Transmisi

Informasi penting dikirim melalui koneksi aman dan pendistribusiannya harus dengan persetujuan dari pemilik informasi tersebut. Begitu pula dengan dalam bentuk *hard copy*.

d) Deklasifikasi

Informasi penting akan dikenakan deklasifikasi namun pada tingkat yang rendah.

e) Pemusnahan

Informasi yang termasuk dalam klasifikasi penting perlu dikontrol seperti merobek-robek. Bila memungkinkan barang-barang harus dihanguskan.

f) Proses Pendistribusian Informasi

Aset informasi penting tidak dapat bebas didistribusikan. Aset terbatas dapat didistribusikan hanya setelah mendapat izin dari pihak PT Infomedia Nusantara, tanpa harus meminta izin kepada pemilik aset informasi sebenarnya.


g) *Login* Keamanan

Diperlukan perizinan kepada pihak PT Infomedia Nusantara yang berkaitan dengan kebaruan dan penggunaan informasi.

iii) **Rahasia**

a) Proses Pengamanan

Untuk mengakses informasi tidak diizinkan membawa barang-barang seperti alat tulis, kamera, dan alat perekam lainnya pada saat mengakses aset informasi sangat rahasia. Selain itu perlu adanya pendampingan pada saat

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	12

akan mengakses aset informasi tersebut.

b) Penyimpanan

Informasi Rahasia harus disimpan di daerah yang sangat aman dan tidak boleh ada akses publik. Hanya personel tertentu yang dapat mengakses informasi tersebut dan dengan perizinan yang tertulis disertakan maksud tujuan dari peminjaman informasi serta harus ditandatangani minimal oleh Pimpinan terkait untuk mengakses informasi tersebut.

c) Transmisi

Informasi Rahasia, tidak boleh dikirim melalui koneksi dan harus dalam bentuk *hard copy* dan pendistribusiannya harus dengan persetujuan dari pemilik informasi serta harus dengan surat izin ataupun keterangan dari pihak yang akan mengakses. Begitu pula dalam bentuk *hard copy* harus mendapatkan izin dari pemilik informasi disertakan dengan surat perizinan yang menyatakan tujuan penggunaan informasi serta harus ditandatangani minimal oleh Manajemen Puncak PT Infomedia Nusantara.

d) Deklasifikasi

Informasi Rahasia deklasifikasi karena sudah berada pada tingkat tinggi dalam klasifikasi aset informasi.

e) Pemusnahan

Informasi yang termasuk dalam klasifikasi Rahasia harus dimusnahkan dengan cara dibakar.

f) Proses Pendistribusian Informasi

Aset informasi Rahasia didistribusikan sangat terbatas dan hanya kepada pihak yang diizinkan oleh pemilik informasi yang dapat mengaksesnya.


g) *Login* Keamanan

Terkait dengan proyek informasi sangat rahasia tidak boleh dipinjamkan untuk dibawa keluar dari area aman. Hanya diizinkan untuk dibaca pada area aman dan sebelumnya harus mendapatkan izin terlebih dahulu dari pihak pemegang informasi dan pihak pemegang proyek.

## 4.6 Pengendalian Akses

### 4.6.1 Prasyarat Bisnis Dalam Pengendalian Akses

Proses ini bertujuan untuk mengendalikan akses kepada seluruh personil Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* yg dikelola PT Infomedia Nusantara dan pihak ketiga yang bekerja di PT Infomedia Nusantara untuk pengamanan informasi PT Infomedia Nusantara.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	13

#### a) Kebijakan pengendalian hak akses


Aturan Kebijakan:

- (1) Pemberian hak akses terhadap Informasi dan sistem informasi harus disesuaikan dengan kewenangan yang dimiliki dari pihak yang akan mengakses dengan memperhatikan prinsip *need to know* dan *need to use*.
- (2) Pemetaan antara hak akses ke informasi dan sistem informasi, dengan tugas pekerjaan (*job role*) personil perlu didokumentasikan secara sebagai panduan dasar pemberian hak akses.
- (3) Akses ke sistem informasi wajib menggunakan *User ID* yang bersifat *unique* dan *password*.
- (4) Hak akses khusus (*privileged access rights*), seperti administrator sistem perlu teridentifikasi dan pemegang hak tersebut perlu terdokumentasikan.
- (5) Mekanisme untuk pengajuan, otorisasi, pengadministrasian, pemantauan dan peninjauan hak akses, perlu didokumentasikan secara formal.
- (6) Peninjauan terhadap pemetaan hak akses dan alokasi hak akses perlu dilakukan secara berkala, paling sedikit satu kali dalam 6 (enam) bulan.

#### b) Akses Ke Jaringan Dan Layanan Jaringan

Aturan Kebijakan:

- (1) Perangkat komputer yang terhubung ke jaringan dan layanan jaringan PT Infomedia Nusantara harus dilengkapi dengan mekanisme pengendalian akses pada sistem operasinya.
- (2) Akses ke segmentasi jaringan perlu dibatasi sesuai dengan tugas dan tanggung jawab operasional pengguna.
- (3) Pemetaan antara segmentasi jaringan dengan pengguna jaringan perlu ditetapkan dan didokumentasikan.
- (4) Akses ke segmentasi jaringan dimana terdapat perangkat sistem informasi kritis (*server farm* atau *storage farm*) harus dikendalikan dan dibatasi sesuai dengan kebutuhan dari pengguna.
- (5) Akses ke jaringan nirkabel (Wifi) perlu diamankan dengan menggunakan *password* yang sesuai dengan kebijakan manajemen *password* yang berlaku.
- (6) Perangkat milik pribadi diperkenankan untuk terhubung ke jaringan internal PT Infomedia Nusantara dengan ijin Manajemen PT Infomedia Nusantara.
- (7) Semua akses ke perangkat jaringan PT Infomedia Nusantara hanya dapat

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	14

dilakukan oleh administrator jaringan yang telah mendapatkan otorisasi dari Manager SDS PT Infomedia Nusantara.

- (8) Akses ke jaringan internal secara *remote* harus dikontrol dan diamankan.
- (9) Akses ke jaringan internal secara *remote* harus mendapatkan persetujuan dari Manager SDS PT Infomedia Nusantara.
- (10) Akses ke jaringan internal secara *remote* oleh pihak ketiga harus dibatasi jangka waktunya hanya pada saat munculnya kebutuhan akses secara *remote*.
- (11) Penggunaan jaringan dan layanan jaringan perlu dipantau dan ditinjau berkala melalui proses *review* dari *audit log*.
- (12) Jaringan dan layanan jaringan di Layanan Information Technology Directorate yang meliputi pengembangan infrastruktur dan sistem yang dikelola PT Infomedia Nusantara dapat menerapkan teknologi pengamanan, seperti otentikasi dan enkripsi jaringan.

#### 4.7 Pengelolaan Akses Pengguna


Proses ini bertujuan untuk memastikan akses pengguna ke sistem informasi merupakan akses yang telah terotorisasi dan mencegah akses yang tanpa otorisasi ke dalam sistem informasi. Hal ini mencakup semua tahapan mulai registrasi *account* pengguna baru sampai dengan penghapusan *account* dari pengguna yang tidak memerlukan lagi akses ke dalam sistem informasi.

##### 4.7.1 Pendaftaran dan penghapusan pengguna (*user*) sistem informasi

Aturan Kebijakan:

- (1) Proses registrasi dan deregistrasi pengguna ke sistem informasi PT Infomedia Nusantara harus ditetapkan secara formal dan diterapkan secara konsisten.
- (2) Hal ini mencakup proses permohonan, persetujuan dan pembuatan / penghapusan *user ID*
- (3) *User ID* harus bersifat unik dan dapat dipetakan dengan identitas pengguna.
- (4) Penggunaan *user ID* secara *sharing* harus sangat dibatasi.
- (5) Penggunaan *user ID* secara *sharing* hanya dapat diizinkan apabila terdapat alasan operasional yang tidak dapat dihindari dan telah disetujui oleh kepala unit kerja yang membidangi keamanan sistem informasi di PT Infomedia Nusantara.
- (6) Segera mencabut atau menonaktifkan *User ID* personil PT Infomedia Nusantara yang telah berganti fungsi pekerjaan atau telah meninggalkan lingkungan PT Infomedia Nusantara.



	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	15

(7) Seluruh proses pendaftaran dan pencabutan pengguna harus didokumentasikan dengan baik.

#### 4.7.2 Pemberian Hak Akses Pengguna

Aturan Kebijakan:


- (1) Permintaan untuk pemberian hak akses pengguna ke sistem informasi harus disetujui oleh atasan dari pengguna dan pemilik dari informasi atau sistem informasi.
- (2) Persetujuan pemberian hak akses pengguna perlu menimbang kebutuhan operasional pekerjaan yang telah didokumentasikan dalam pemetaan hak akses.
- (3) Pemberian hak akses hanya dapat dilakukan setelah persetujuan dalam butir (1) telah diberikan.
- (4) Seluruh proses pemberian hak akses pengguna harus terdokumentasi dengan baik.

#### 4.7.3 Pengelolaan Hak Akses Khusus (*Privileged Access Rights*)

Aturan Kebijakan:

- (1) Hak akses khusus adalah hak akses ke informasi maupun sistem informasi dengan kemampuan (*privilege*) yang lebih tinggi dibandingkan hak akses lainnya. Sebagai contoh adalah hak akses dengan kemampuan (*privilege*) administrator atau *full access*.
- (2) Pemberian dan penggunaan hak akses khusus harus dibatasi dan dikendalikan kepada personil dengan tugas dan tanggung jawab yang sesuai.
- (3) Proses otorisasi dan catatan dari semua hak akses khusus yang diberikan harus didokumentasikan.
- (4) Hak akses khusus perlu diberikan dalam format *user ID* yang berbeda dengan hak akses biasa dan bersifat sementara.
- (5) Penggunaan hak akses khusus secara *sharing* harus sangat dibatasi.
- (6) Penggunaan hak akses khusus secara *sharing* hanya dapat diizinkan apabila terdapat alasan operasional yang tidak dapat dihindari dan telah disetujui oleh kepala unit kerja yang membidangi keamanan sistem informasi di PT Infomedia Nusantara.
- (7) Penggunaan hak akses khusus secara *sharing* harus dikendalikan antara lain dengan kontrol-kontrol berikut:
  - a. Penggantian *password* secara berkala;
  - b. Penggantian *password* segera setelah salah satu pemegang hak tersebut tidak bekerja lagi atau mengalami mutasi kerja.



	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	16

- (8) Penggunaan hak akses khusus harus dimonitor untuk memastikan tidak adanya akses tanpa ijin.
- (9) Hak akses khusus dengan tujuan untuk pelaksanaan audit terhadap sistem informasi harus diberikan dengan kemampuan (*privilege*) *read only*.

#### 4.7.4 Pengelolaan Informasi Otentikasi Rahasia Milik Pengguna


Aturan Kebijakan:

- (1) Informasi otentikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentikasikan seorang pengguna. Contoh dari informasi ini adalah *password*, *smartcard*, *token* atau PIN.
- (2) Pengguna harus memahami kewajiban mereka untuk menjaga keamanan dari informasi otentikasi rahasia yang mereka miliki.
- (3) Pengguna dilarang untuk memberikan informasi otentikasi rahasia miliknya kepada pihak lain.
- (4) Untuk informasi otentikasi dalam bentuk *password*, apabila pengguna terpaksa memberikan informasi tersebut kepada pihak lain, maka pengguna tersebut harus mengganti informasi tersebut pada kesempatan pertama.
- (5) Pemberian informasi otentikasi dalam bentuk *password* untuk pertama kali dapat menggunakan *password* sementara yang harus diganti oleh pengguna setelah proses *login* untuk pertama kalinya.
- (6) Informasi otentikasi yang bersifat *default* dari *vendor* perangkat atau aplikasi sistem informasi harus diganti pada saat instalasi perangkat atau aplikasi tersebut.

#### 4.7.5 Peninjauan Terhadap Hak Akses Pengguna

Aturan Kebijakan:

- (1) Peninjauan hak akses dilakukan untuk memastikan kesesuaian hak akses yang dialokasikan dengan kondisi terkini dari pengguna, terkait kewenangan dan status kepegawaian, dari pengguna.
- (2) Pemilik atau administrator dari perangkat dan aplikasi sistem informasi harus melakukan peninjauan terhadap hak akses pengguna secara berkala minimal satu kali dalam 6 (enam) bulan atau apabila terdapat perubahan pada:
  - a. Status kepegawaian seperti mutasi atau terminasi.
  - b. Proses bisnis organisasi.
  - c. Proses Sistem informasi.
- (3) Hak akses khusus (*privileged*) harus ditinjau secara *reguler* dengan jangka waktu setiap 6 (enam) bulan.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	17

#### 4.7.6 Perubahan atau Pencabutan Hak Akses

Aturan Kebijakan:

- (1) Pengguna yang mengalami perubahan fungsi pekerjaan/mutasi harus segera melaporkan perubahan tersebut dan mengajukan permintaan perubahan hak akses paling lambat 7 hari setelah perubahan/mutasi tersebut.
- (2) Perubahan hak akses hanya dapat dilakukan setelah persetujuan dari atasan pengguna dan pemilik informasi atau sistem informasi dengan memperhatikan pemetaan hak akses pengguna.
- (3) Pencabutan hak akses pengguna dapat dilakukan:
  - a. Atas permintaan dan persetujuan dari atasan pengguna dan pemilik sistem informasi;
  - b. Secara otomatis, apabila pengguna sudah tidak bekerja lagi di lingkungan PT Infomedia Nusantara.
  - c. Sesuai hasil peninjauan hak akses pengguna yang minimal dilakukan 6 (enam) bulan sekali sesuai ruang lingkup implementasi SMKI.
- (4) Hak akses untuk pengguna yang sudah tidak bekerja lagi di lingkungan PT Infomedia Nusantara harus dicabut atau di-*suspend* satu hari setelah hari terakhir pengguna tersebut.
- (5) Seluruh proses perubahan dan pencabutan hak akses pengguna harus terdokumentasi dengan baik.


#### 4.8 Tanggung Jawab Pengguna (User)

Kontrol-kontrol ini bertujuan agar pengguna memiliki pemahaman mengenai penggunaan akses secara aman.

##### 4.8.1 Penggunaan Informasi Otentikasi Pengguna yang Bersifat Rahasia

Aturan Kebijakan:

- (1) Informasi otentikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentikasikan seorang pengguna. Contoh dari informasi ini adalah *password, smartcard, token* atau PIN.
- (2) Setiap pengguna wajib menggunakan Informasi otentikasi rahasia dalam proses otentikasi ke perangkat dan aplikasi sistem informasi organisasi.
- (3) Setiap pengguna wajib menjaga kerahasiaan informasi otentikasi rahasia dan menghindari menyimpan informasi otentikasi rahasia di tempat terbuka atau tempat yang tidak memiliki pengamanan yang memadai.
- (4) Setiap personil Layanan *Customer Relationship Management* dan Layanan *Shared Service Operations* yang dikelola PT Infomedia Nusantara wajib

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	18

mengganti informasi otentikasi rahasia apabila ada indikasi adanya penyalahgunaan atau kebocoran.

- (5) Apabila *password* digunakan sebagai informasi otentikasi rahasia, maka catatan yang berisi *password* tidak boleh disimpan pada tempat terbuka atau tanpa pengamanan yang memadai.
- (6) Apabila *password* digunakan sebagai informasi otentikasi rahasia, maka *password* harus berkualitas dengan karakteristik sebagai berikut:
  - Panjang minimal karakter *password* pada perangkat dan aplikasi sistem informasi yang digunakan adalah 6 (enam) karakter;
  - Menggunakan kombinasi huruf dan angka dan sedapat mungkin menggunakan karakter khusus (*special character*), seperti: !\$%#\*, kecuali apabila perangkat atau aplikasi tidak memungkinkan.
  - Penggunaan Perangkat atau aplikasi yang tidak dimungkinkan mengikuti kebijakan penggunaan *password* yang berkualitas harus mendapatkan persetujuan dari Koordinator SMKI dengan mempertimbangkan kebutuhan operasional, risiko dan kontrol kompensasi.
- (7) *Password* tidak boleh sama dengan *User ID* dan tidak berdasar pada sesuatu yang mudah ditebak misalnya: nama, nomor telepon, tanggal lahir, nama anggota keluarga, nama/identitas perusahaan.
- (8) Mengganti *password* secara berkala setiap 6 (enam) bulan dengan menghindari menggunakan *password* yang sudah pernah digunakan.
- (9) Setiap pengguna wajib menjaga kerahasiaan *password* dan tidak diperkenankan memberikan *password*-nya kepada orang lain dan atau menggunakan *password* milik orang lain.


#### 4.9 Pengendalian Akses Informasi dan Aplikasi

Proses ini bertujuan untuk mencegah akses tanpa wewenang ke sistem di Layanan Information Technology Directorate yang meliputi pengembangan infrastruktur dan sistem yang dikelola PT Infomedia Nusantara Dengan membatasi akses ke sistem jaringan.

##### 4.9.1 Pembatasan akses informasi

Aturan Kebijakan:

- (1) Akses ke informasi oleh pengguna harus dibatasi sesuai dengan tugas dan tanggung jawabnya.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	19

#### 4.9.2 Prosedur *log-on secara aman*

Aturan Kebijakan:

(1) Akses ke sistem operasi harus dikontrol dengan menggunakan mekanisme *secure log-on* yang meliputi:

- Tidak memberikan informasi bantuan yang dapat menyebabkan *log-on* tanpa ijin.
- Membatasi jumlah kesalahan dalam percobaan *log-on* sebanyak 3 (tiga) kali.
- Tidak menampilkan karakter *password* pada saat *log-on*. Tampilan karakter *password* dapat diganti dengan simbol.
- Sistem dan/atau aplikasi hanya ditampilkan setelah *log-on* berhasil dilaksanakan;
- Menampilkan notifikasi peringatan bahwa computer hanya boleh diakses oleh pihak yang berwenang;
- Pembatasan lama waktu yang dibutuhkan untuk melakukan satu kali proses *log-on*, sebelum proses *log-on* ditampilkan kembali;
- *Password* yang dikirim lewat jaringan harus dienkripsi terlebih dahulu

#### 4.9.3 Sistem Pengelolaan *Password*

Aturan Kebijakan:


(1) Sistem pengelolaan password harus dapat:

- a. Memastikan penggantian *password* secara reguler yaitu maksimal 6 (enam) bulan sekali.
- b. Memastikan kualitas *password* sesuai dengan aturan dalam kebijakan ini.
- c. Memastikan penyimpanan dan pengiriman informasi *password* secara aman.

#### 4.9.4 Penggunaan Program Utilisasi Khusus.

Aturan Kebijakan:

- (1) Penggunaan *system utility programs* yang berpotensi dapat mengambil alih pengendalian perangkat dan aplikasi sistem informasi harus dibatasi dan dikendalikan secara ketat.
- (2) *Administrator* harus melakukan proses identifikasi dan otorisasi untuk seluruh *system utilities* yang digunakan.
- (3) Permintaan terhadap penggunaan *system utility programs* harus melalui *Helpdesk*

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	20

#### 4.9.5 Pengendalian akses ke kode program (*source code*).

Aturan Kebijakan:

- (1) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
- (2) Akses oleh Pengelola TIK ke kode program (*source code*) dan *library* harus dibatasi;
- (3) Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program (*source code*) kepada programmer hanya dapat dilakukan setelah melalui proses otorisasi;
- (4) *Listing* program harus disimpan dalam area yang aman;
- (5) Pemeliharaan dan penyalinan kode program (*source code*) *library* harus mengikuti prosedur pengendalian perubahan.

#### 4.10 Pengendalian Kriptografi

Proses ini bertujuan untuk menjaga kerahasiaan, keaslian dan integritas informasi dengan menggunakan teknologi kriptografi.

##### 4.10.1 Kebijakan penggunaan kriptografi


Aturan Kebijakan:

- (1) Penggunaan kriptografi perlu dipertimbangkan untuk menjaga kerahasiaan, keaslian dan integritas informasi;
- (2) Penggunaan kriptografi perlu mempertimbangkan kekuatan dari algoritma kriptografi.
- (3) Penggunaan kriptografi perlu dipertimbangkan untuk melindungi informasi pada perangkat *mobile* atau *removable media*.
- (4) Penggunaan teknologi kriptografi harus ditinjau terlebih dahulu oleh kepala unit kerja yang membidangi keamanan informasi.
- (5) Penggunaan teknologi kriptografi harus disetujui terlebih dahulu oleh kepala unit kerja yang membidangi teknologi informasi.

##### 4.10.2 Manajemen dari *key* untuk kebutuhan kriptografi

Aturan Kebijakan:

- (1) Seluruh *key* kriptografi harus dilindungi dari modifikasi, kehilangan serta kerusakan.
- (2) Pengelolaan *key* kriptografi harus menggunakan prinsip *dual custody*, dimana *key* kriptografi tidak boleh diketahui oleh hanya satu personil saja.
- (3) Untuk *key* kriptografi dalam bentuk *cleartext*, maka pengiriman informasi

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	21

dan *key* yang digunakan untuk mengenkripsi informasi tersebut harus dilakukan dalam media komunikasi yang berbeda. Sebagai contoh, pengiriman dokumen elektronik dilakukan melalui media *email* sedangkan pengiriman *password* yang digunakan untuk mengenkripsi dokumen tersebut dilakukan melalui SMS atau telepon.

- (4) Pemantauan harus dilakukan terhadap kunci kriptografi yang diterapkan minimal 1 kali dalam setahun.

#### 4.11 Wilayah yang Aman

Wilayah yang aman diperoleh melalui pembatasan wilayah dengan menggunakan pembatasan fisik untuk mencegah akses fisik tanpa izin yang dapat menimbulkan gangguan, kehilangan atau kerusakan terhadap informasi milik PT Infomedia Nusantara.

##### 4.11.1 Perimeter Keamanan Fisik

Aturan Kebijakan:

- (1) Pembatasan wilayah dengan pembatas secara fisik harus digunakan untuk melindungi area yang berisi informasi dan atau fasilitas pengolahan informasi.
- (2) Pengamanan fisik ruang Operasional PT Infomedia Nusantara Mengacu kepada klasifikasi wilayah masing-masing ruangan dengan menggunakan pembatas dan pengendalian akses fisik.

##### 4.11.2 Pengendalian akses fisik


Aturan Kebijakan:

- (1) Akses fisik ke wilayah aman (operasional) harus dikendalikan untuk menjamin tidak adanya akses tanpa izin.
- (2) Tamu atau pihak ketiga yang datang ke area kerja Operasional PT Infomedia Nusantara harus tetap didampingi atau diawasi.
- (3) Tamu atau pihak ketiga yang mengakses area kritikal di PT Infomedia Nusantara Hanya untuk personil yang mempunyai kewenangannya dan diotorisasi oleh Pimpinan penanggung jawab di ruang tersebut dan harus diawasi dan didampingi oleh pegawai di ruangan tersebut.

##### 4.11.3 Pengamanan Ruang Kantor dan Fasilitasnya

Aturan Kebijakan:

- (1) Ruang kerja dan fasilitas pada Operasional PT Infomedia Nusantara perlu diberikan pengamanan secara memadai dengan mempertimbangkan pemisahan dari wilayah akses umum

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	22

- (2) Untuk area kritis di Operasional PT Infomedia Nusantara tidak dipasang informasi/petunjuk lokasi yang jelas.
- (3) Apabila memungkinkan, fasilitas yang digunakan untuk pemrosesan dan penyimpanan informasi sensitif sebaiknya terpisah dengan fasilitas yang digunakan untuk pekerjaan sehari-hari.
- (4) Area kerja Organisasi dibagi menjadi tiga:
  - Area level 1, yaitu area yang dapat diakses oleh personil atau tamu tanpa pengaturan khusus. Contohnya *lobby* dan ruang rapat.
  - Area level 2, yaitu area di mana hanya personil dan tamu yang terdaftar yang memperoleh akses sesuai ketentuan yang ada. Contohnya ruang kerja.
  - Area level 3, yaitu area aman atau area yang hanya dapat diakses oleh personil dan tamu yang sudah diotorisasi. Contohnya ruang operasional, *server room*, ruang pimpinan terkait.

#### 4.11.4 Perlindungan Terhadap Ancaman Eksternal dan Lingkungan

Aturan Kebijakan:

- (1) Peralatan pemadam kebakaran yang memadai harus tersedia pada tempat yang sesuai.
- (2) Khusus ruangan kritis pada Operasional PT Infomedia Nusantara Menggunakan peralatan pemadam kebakaran yang bersifat *non-liquid*.

#### 4.11.5 Bekerja di Area Aman (Operasional)

Aturan Kebijakan:


- (1) Pekerjaan yang dilakukan oleh pihak ketiga di area kritis di lingkungan Operasional PT Infomedia Nusantara harus selalu diawasi oleh personil penanggung jawab area tersebut untuk menghindari kegiatan yang tidak diinginkan.
- (2) Setiap personil dan pihak ketiga dilarang membawa makanan, minuman, rokok, dan barang berbahaya ke dalam wilayah tertutup.
- (3) Setiap personil dan pihak ketiga yang memasuki wilayah tertutup tidak diperkenankan membawa peralatan *visual recording (camera, handphone berkamera)* tanpa otorisasi dari pimpinan yang berwenang.

#### 4.11.6 Area untuk *delivery* dan *loading*

Aturan Kebijakan:

- (1) Akses di wilayah *loading area* yang dapat memasuki wilayah Operasional PT



	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	23

Infomedia Nusantara harus diamankan untuk menghindari akses tanpa ijin.

#### 4.12 Perangkat

Pengamanan ini diperlukan untuk mencegah kehilangan, kerusakan, pencurian terhadap aset atau gangguan terhadap aktivitas .

##### 4.12.1 Perlindungan dan penempatan peralatan

Aturan Kebijakan:

- (1) Perangkat pengolahan informasi yang dianggap kritikal perlu ditempatkan secara aman termasuk membatasi sudut pandang untuk mengurangi orang yang tidak berkepentingan yang dapat melihat informasi yang ditampilkan.

##### 4.12.2 Sarana Pendukung

Aturan Kebijakan:  **CC TELKOM**

- (1) Semua sarana pendukung seperti *power supply*, genset, lampu darurat, dan *air conditioner* harus tersedia untuk mendukung kegiatan Operasional PT Infomedia Nusantara dan dipelihara secara berkala.

##### 4.12.3 Pengamanan pengkabelan

Aturan Kebijakan:

- (1) Kabel listrik dan jaringan komunikasi harus terlindungi dan tidak diletakkan di area publik sehingga tidak mengalami kerusakan akibat ketidaksengajaan oleh personil maupun gigitan binatang pengerat.
- (2) Penandaan kabel digunakan di Ruang *Server Jaringan* untuk mempermudah penanganan apabila terjadi masalah dan menghindari kesalahan dan didokumentasikan dengan baik.

##### 4.12.4 Pemeliharaan peralatan

Aturan Kebijakan:


- (1) Peralatan sistem informasi seperti perangkat keras dan jaringan komunikasi, serta sarana pendukung harus dipelihara untuk menjamin ketersediaan dari peralatan tersebut secara terus menerus.

##### 4.12.5 Pemindahan Peralatan Milik Operasional PT Infomedia Nusantara

Aturan Kebijakan:

- (1) Peralatan, informasi, maupun perangkat lunak tidak boleh dibawa keluar



	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	24

wilayah Operasional PT Infomedia Nusantara tanpa adanya izin dari Pimpinan terkait di PT Infomedia Nusantara.

#### 4.12.6 Pengamanan peralatan di luar wilayah PT Infomedia Nusantara

Aturan Kebijakan:

- (1) Penggunaan peralatan pengolahan informasi diluar wilayah Operasional PT Infomedia Nusantara mempertimbangkan kebutuhan penggunaan aset tersebut.
- (2) Aset TI yang bersifat *portable* seperti *notebook* yang dibawa ke luar area kantor tidak boleh ditinggalkan di area publik tanpa pengamanan yang memadai dengan kabel pengunci (*cable lock*) serta *password*.

#### 4.12.7 Pemusnahan atau Penggunaan Kembali Peralatan Secara Aman

Aturan Kebijakan:

- (1) Seluruh Aset TI yang akan dimusnahkan atau digunakan kembali harus diperiksa dan dipastikan bahwa tidak ada lagi data sensitif yang tersimpan dalam perangkat sehingga tidak dimungkinkan lagi untuk mengambil informasi yang sebelumnya terkandung di perangkat tersebut.

#### 4.12.8 Perlindungan untuk perangkat yang tidak dalam pengawasan


Aturan Kebijakan:

- (1) Pengguna harus memastikan aset yang sedang tidak digunakan telah terlindungi dengan baik dengan menghentikan (*terminate*) *session* aktif terhadap sistem setelah selesai digunakan.
- (2) Pengguna harus mengunci layar sistem operasi pada komputernya (*screen lock*) apabila meninggalkan komputernya.
- (3) Komputer perlu dilindungi dengan fitur penguncian layar secara otomatis (*screen saver lock*) apabila tidak aktifitas pada layar komputer selama 5 menit.

#### 4.12.9 Clear desk dan clear screen

Aturan Kebijakan:

- (1) Seluruh personil PT Infomedia Nusantara harus menerapkan *clear desk* dan *clear screen* terkait dengan keamanan informasi yang rahasia atau sensitif.
- (2) Semua informasi sensitif yang berbentuk *hardcopy* atau yang tersimpan dalam media penyimpanan dalam lemari yang terkunci.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	25

- (3) Komputer harus di *log-off*/mengunci layar komputernya apabila sedang tidak digunakan.
- (4) Menerapkan fitur *log-off*/mengunci layar secara otomatis pada laptop atau komputer (PC) yang digunakan untuk bekerja.
- (5) Memindahkan dengan segera dokumen yang mengandung informasi sensitif dari mesin *printer*.

#### 4.13 Perlindungan terhadap *Malware*

Pengguna sistem informasi pada Operasional PT Infomedia Nusantara perlu memahami bahaya dari *Malware* dan mengetahui bagaimana mencegah serta menangani adanya *Malware*.

##### 4.13.1 Pengendalian Terhadap *Malware*

Aturan Kebijakan:  **CC TELKOM**


- (1) Kontrol terhadap *Malware* dapat dilakukan melalui pendeteksian dan pencegahan serangan *Malware* dan pemulihan setelah terjadi serangan dari *Malware*.
- (2) Personil Operasional PT Infomedia Nusantara harus melindungi sistem informasi dari serangan *Malware* dengan tidak meng-*install* perangkat lunak bajakan dan/atau perangkat lunak yang tidak sesuai dengan kebutuhan kerja.
- (3) Setiap perangkat seperti *PC* dan *Notebook*, dan *server* harus menggunakan program *antivirus* untuk mencegah bahaya *Malware* (*virus*, *worm*, *trojan*).
- (4) Setiap personil Operasional PT Infomedia Nusantara harus memastikan bahwa setiap file dokumen elektronis yang berasal dari media penyimpanan atau jaringan, termasuk *email* dan *internet*, tidak mengandung *virus* dengan melakukan *scanning* terhadap *file* atau program tersebut sebelum mengakses atau menggunakan.
- (5) *Update* dan *scanning* rutin harus dilakukan secara otomatis untuk memastikan kemampuan program antivirus untuk mendeteksi dan menangani *malware* pada komputer dan media penyimpanan.

#### 4.14 *Back-up*

Proses *back-up* diperlukan untuk menjamin integritas dan ketersediaan informasi serta fasilitas pengolahan informasi.

##### 4.14.1 *Back-up* Informasi

Aturan Kebijakan:

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	26

- (1) Informasi elektronik yang bersifat rahasia atau kritis (memiliki tingkat integritas dan ketersediaan tinggi) harus memiliki *back-up*, sehingga apabila data/informasi utama tidak dapat dibaca, rusak, dan lain sebagainya, masih dapat menggunakan data *back-up*.
- (2) Frekuensi dan tingkat *back-up* (penuh atau parsial) disesuaikan dengan kebutuhan kritikalitas bisnis.
- (3) Hasil *back-up* harus disimpan pada tempat yang aman dan diusahakan ditempatkan diluar lokasi utama dan diberikan perlindungan secara fisik dan lingkungan yang memadai.
- (4) Media *back-up* harus diuji secara berkala melalui uji *restore* untuk memastikan media tersebut dapat berfungsi dengan baik pada saat dibutuhkan.
- (5) Masa retensi dari *back-up* informasi tergantung dari tingkat kritikalitas suatu informasi dan sistem yang dioperasikan pada Operasional PT Infomedia Nusantara.

#### 4.15 Pengelolaan *technical vulnerability*

Manajemen *technical vulnerabilities* harus diimplementasikan secara efektif, sistematis, dan secara rutin dengan disertai pengukuran efektivitasnya.

##### 4.15.1 Pengendalian terhadap kelemahan teknis (*technical vulnerability*)


Aturan Kebijakan:

- (1) *Administrator* sistem informasi perlu mencari informasi terkini tentang *technical vulnerability* pada sistem informasi PT Infomedia Nusantara.
- (2) Informasi terkini tentang *technical vulnerability* dapat diperoleh dari proses *vulnerability assessment* atau dari forum terkait keamanan informasi.
- (3) Informasi mengenai *technical vulnerability* harus segera ditindaklanjuti untuk menghilangkan atau mengurangi dampaknya.

##### 4.15.2 Pembatasan instalasi perangkat lunak

Aturan Kebijakan:

- (1) Instalasi atau modifikasi perangkat lunak harus dikendalikan untuk mengurangi risiko *downtime* pada sistem informasi
- (2) *Software* atau aplikasi yang boleh di-install adalah *software* yang hanya diperbolehkan oleh PT Infomedia Nusantara. Daftar *software* dapat dilihat pada lampiran.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	27

#### 4.16 Pertimbangan dalam audit sistem informasi

Proses ini bertujuan untuk memaksimalkan efektivitas dari proses audit dan meminimalkan adanya campur tangan pada proses audit.

##### 4.16.1 Pengendalian terhadap audit sistem informasi

Aturan Kebijakan:

- (1) Auditor sistem informasi perlu merencanakan proses audit yang melibatkan pemeriksaan sistem operasional. Perencanaan ini meliputi:
  - Ruang lingkup dari pemeriksaan audit harus disepakati dengan pihak manajemen terkait.
  - Akses audit ke sistem informasi maupun informasi hanya dibatasi dengan hak akses *read only*.
  - Pemantauan dan pencatatan seluruh akses ke sistem informasi untuk menghasilkan *reference trail*.
  - Pelaksana audit harus memiliki independensi dari aktivitas yang diaudit.
  - Perlu dilakukan audit sistem informasi secara berkala minimal 1 tahun sekali.

## 5 Keamanan Komunikasi


### 5.1 Manajemen Keamanan Jaringan

Keamanan jaringan perlu dikelola dengan baik untuk menjamin perlindungan terhadap informasi yang dikirimkan melalui jaringan dan infrastruktur pendukung jaringan lainnya. Pengelolaan keamanan jaringan perlu mempertimbangkan perlindungan informasi sensitif melalui jaringan publik.

#### 5.1.1 Pengendalian jaringan

Aturan Kebijakan:

- (1) Akses ke perangkat jaringan dan sistem pendukungnya hanya dapat dilakukan oleh administrator jaringan atau pihak lainnya yang telah mendapat izin dari administrator jaringan.
- (2) Jaringan dan perangkat jaringan PT Infomedia Nusantara perlu dipantau secara kontinu.
- (3) Akses ke jaringan PT Infomedia Nusantara Hanya diberikan kepada perangkat milik PT Infomedia Nusantara.
- (4) Konfigurasi jaringan PT Infomedia Nusantara perlu dirancang sedemikian rupa sehingga kegagalan pada satu jalur komunikasi tidak akan membuat terhentinya layanan jaringan komunikasi.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	28

(5) Akses dari jaringan eksternal ke jaringan internal PT Infomedia Nusantara harus melalui proses otentikasi.

(6) Akses dari jaringan eksternal ke jaringan internal PT Infomedia Nusantara perlu mempertimbangkan teknologi kriptografi pada jaringan, seperti teknologi VPN.

### 5.1.2 Keamanan Layanan Jaringan

Aturan Kebijakan:

- (1) Layanan jaringan mencakup layanan sistem informasi yang menggunakan jaringan komunikasi PT Infomedia Nusantara. Hal ini mencakup namun tidak terbatas pada, email, internet, aplikasi berbasis *web*.
- (2) Setiap akses ke layanan jaringan PT Infomedia Nusantara harus melalui proses otentikasi.
- (3) Penggunaan layanan jaringan perlu dipantau secara kontinu.
- (4) Setiap layanan jaringan perlu dilengkapi dengan fitur keamanan untuk menjaga aspek kerahasiaan dan integritas informasi.


### 5.1.3 Pemisahan (*segregation*) dalam jaringan

Aturan Kebijakan:

- (1) Jaringan internal dan eksternal PT Infomedia Nusantara harus dipisahkan menggunakan *security gateway*. Hal ini mencakup namun tidak terbatas pada penggunaan *firewall*, *filtering router* atau *server*.
- (2) Jaringan internal PT Infomedia Nusantara perlu dipisahkan berdasarkan tingkat kritikalitas perangkat yang terdapat didalam jaringan tersebut dan/atau unit organisasi.
- (3) *Server-server* yang digunakan oleh PT Infomedia Nusantara harus terdapat pada segmentasi jaringan tersendiri yang terpisah dari segmentasi jaringan pengguna.
- (4) *Server-server* yang digunakan untuk kegiatan operasional (*production*) harus dipisahkan dari *server-server* untuk kegiatan pengembangan dan/atau pengujian.
- (5) Pemisahan atau segmentasi dapat dilakukan secara fisik maupun *logical* berdasarkan risiko yang ada.

## 5.2 Pertukaran Informasi

Proses pertukaran informasi perlu diamankan untuk melindungi pertukaran informasi antara Operasional PT Infomedia Nusantara dengan pihak eksternal dari ancaman.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	29

### 5.2.1 Kebijakan dan Prosedur Pertukaran Informasi

Aturan Kebijakan:

- (1) Pertukaran Informasi dengan menggunakan fasilitas *e-mail* harus memperhatikan perlindungan terhadap informasi yang dipertukarkan (dalam bentuk *attachment*) dari salah pengiriman dan perusakan. Jika dimungkinkan menggunakan *password* untuk melindungi kerahasiaan, integritas dan keaslian Informasi yang dipertukarkan.

### 5.2.2 Perjanjian Pertukaran

Aturan Kebijakan:

- (1) PT Infomedia Nusantara harus memastikan adanya perjanjian formal dalam melakukan pertukaran informasi dengan pihak lain untuk memastikan semua pihak yang terlibat melakukan pengamanan informasi dengan memuat hal-hal sebagai berikut :
  - Kesepakatan dalam kesepahaman yang sama terkait keamanan informasi sehingga informasi dapat dilindungi secara memadai
  - Penyimpanan Informasi secara aman dan memadai.
  - Penggunaan sistem pelabelan yang telah disepakati untuk informasi yang sensitif.
  - Penggunaan teknologi *password* yang diperlukan.

### 5.2.3 Pesan Elektronik (*e-mail*)


Aturan Kebijakan:

- (1) Pengiriman informasi milik PT Infomedia Nusantara menggunakan *e-mail* harus dilindungi untuk menghindari kebocoran informasi secara tidak sengaja akibat kesalahan pengiriman dan tanpa ada pengamanan pada *file*.

### 5.2.4 Perjanjian Kerahasiaan

Aturan Kebijakan:

- (1) Setiap personil PT Infomedia Nusantara maupun pihak ketiga yang bekerja untuk PT Infomedia Nusantara harus menyetujui dan menandatangani pernyataan menjaga kerahasiaan informasi yang dituangkan dalam dokumen pernyataan kerahasiaan informasi atau kontrak kerja dan berlaku selama personil aktif di PT Infomedia Nusantara.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	30

### 5.3 Pengamanan pada Proses Pengembangan dan *Support*

Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh *supplier*.

#### 5.3.1 Kebijakan keamanan informasi untuk hubungan dengan *supplier*

Aturan Kebijakan:

- (1) Proses keamanan informasi dengan *supplier* harus disepakati dengan *supplier* terkait dengan akses pemasok untuk aset organisasi.

#### 5.3.2 Menangani keamanan informasi dalam perjanjian dengan *supplier*

Aturan Kebijakan:

- (1) Perjanjian dengan *supplier* harus mencakup klausul kerahasiaan informasi yang disetujui oleh setiap *supplier* (dalam dokumen kontrak atau perjanjian kerjasama)
- (2) Setiap personil *supplier* yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau mengkonfigurasi komponen infrastruktur TI, dan informasi untuk organisasi harus menandatangani perjanjian kerahasiaan informasi.

#### 5.3.3 *Supply Chain* dari teknologi informasi dan komunikasi

Aturan Kebijakan:

- (1) *Supply Chain* dari teknologi informasi dan komunikasi harus mencakup kebutuhan untuk mengatasi resiko terkait dengan keamanan informasi dan layanan teknologi dan produk *supply chain*.


### 5.4 Pengelolaan Pemberian Layanan (*Service Delivery*)

Pengelolaan pemberian layanan bertujuan untuk menjaga tingkat keamanan informasi dan tingkat layanan yang disetujui sesuai dengan perjanjian.

#### 5.4.1 Pemantauan dan Peninjauan Layanan dari *Supplier*

Aturan Kebijakan:

- (1) Pemantauan terhadap layanan yang disediakan oleh Pihak Ketiga meliputi antara lain:
  - Memantau tingkat layanan yang diberikan sesuai dengan perjanjian kerja.
  - Mengkaji laporan yang disampaikan oleh Pihak Ketiga dengan melakukan pertemuan berkala yang dituangkan dalam risalah rapat atau laporan *progress* pelaksanaan pekerjaan pihak ketiga.

	<p style="text-align: center;"><b>Pedoman Kebijakan Keamanan Informasi</b></p>	<b>PT Infomedia Nusantara</b>	
		No. Dokumen	IN.PRO-02
		Versi	1.0
		Klasifikasi	Terbatas
		Tanggal	08 September 2021
		Halaman	31

#### 5.4.2 Mengelola perubahan kepada layanan dari *Supplier*

Aturan Kebijakan:

- (1) Seluruh perubahan terhadap layanan yang diberikan oleh pihak ketiga, termasuk operasional dan pemeliharaan harus dikelola dengan mempertimbangkan sistem yang dijalankan oleh PT Infomedia Nusantara.

#### 5.4.3 Pengamanan Data Pribadi

Aturan Kebijakan:

- (1) PT Infomedia Nusantara perlu melindungi kepemilikan dan kerahasiaan data pribadi personil. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

### 6 PENGKAJIAN DOKUMEN

Dokumen ini dikelola oleh Pengendali Dokumen. Setiap masukan perubahan terhadap prosedur ini harus diajukan kepada Koordinator SMKI. Perubahannya disetujui oleh pemegang kewenangan sesuai ketentuan yang berlaku di PT Infomedia Nusantara.

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

### 7 LAMPIRAN

-