KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

STANDAR OPERASIONAL PROSEDUR
Nomor: SOP/20/VIII/2022/PUSDATIN

TENTANG
PROSEDUR PENANGANAN INSIDEN INFORMASI

DIKELUARKAN DI JAKARTA
TAHUN 2022

BAB I
TUJUAN

1. Tujuan

Prosedur ini merupakan petunjuk dalam manajemen insiden keamanan informasi, yang memiliki tujuan:

a. Memastikan kejadian dan kelemahan keamanan informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi.

b. Memastikan tindakan yang konsisten dan efektif untuk manajemen insiden.

BAB II
RUANG LINGKUP

2. Ruang Lingkup

Prosedur ini mencakup Manajemen Penanganan Insiden yang berkaitan dengan sistem manajemen Keamanan Informasi pada semua tingkatan dan Bidang/Bagian di Pusdatin Kemhan RI.

Prosedur ini mengatur tahapan:

a. Pelaporan Kelemahan dan Penanganan Gangguan Insiden Keamanan Informasi.

b. Tindak Lanjut Pelaporan Gangguan Insiden Keamanan Informasi.

c. Pengumpulan Bukti Setelah Gangguan Insiden Keamanan Informasi.

BAB III
DEFINISI

3. Definisi

a. *Security Hole* adalah kelemahan-kelemahan keamanan terhadap sistem yang ada, baik sistem Teknologi Informasi, sistem fisik maupun sistem manajemen.

b. Keamanan Fisik adalah keamanan yang berkaitan dengan aset fisik. Hal ini termasuk berkaitan dengan penanganan aset fisik mupun akses terhadap aset fisik.

c. Aplikasi Pihak Ketiga adalah aplikasi perangkat lunak yang dibuat oleh pihak di luar perusahaan.

d. Insiden adalah terganggunya sebagian atau keseluruhan aktifitas perusahaan akibat terjadinya sesuatu yang tidak dikehendaki.

e. Kelemahan adalah hal-hal yang berpotensi menyebabkan terjadinya insiden.

f. Pelapor adalah Setiap pihak yang menemukan kelemahan gangguan/ insiden keamanan informasi.

g. Insiden Keamanan Informasi (*Information Security Incident*) adalah insiden yang disebabkan oleh masalah keamanan informasi.

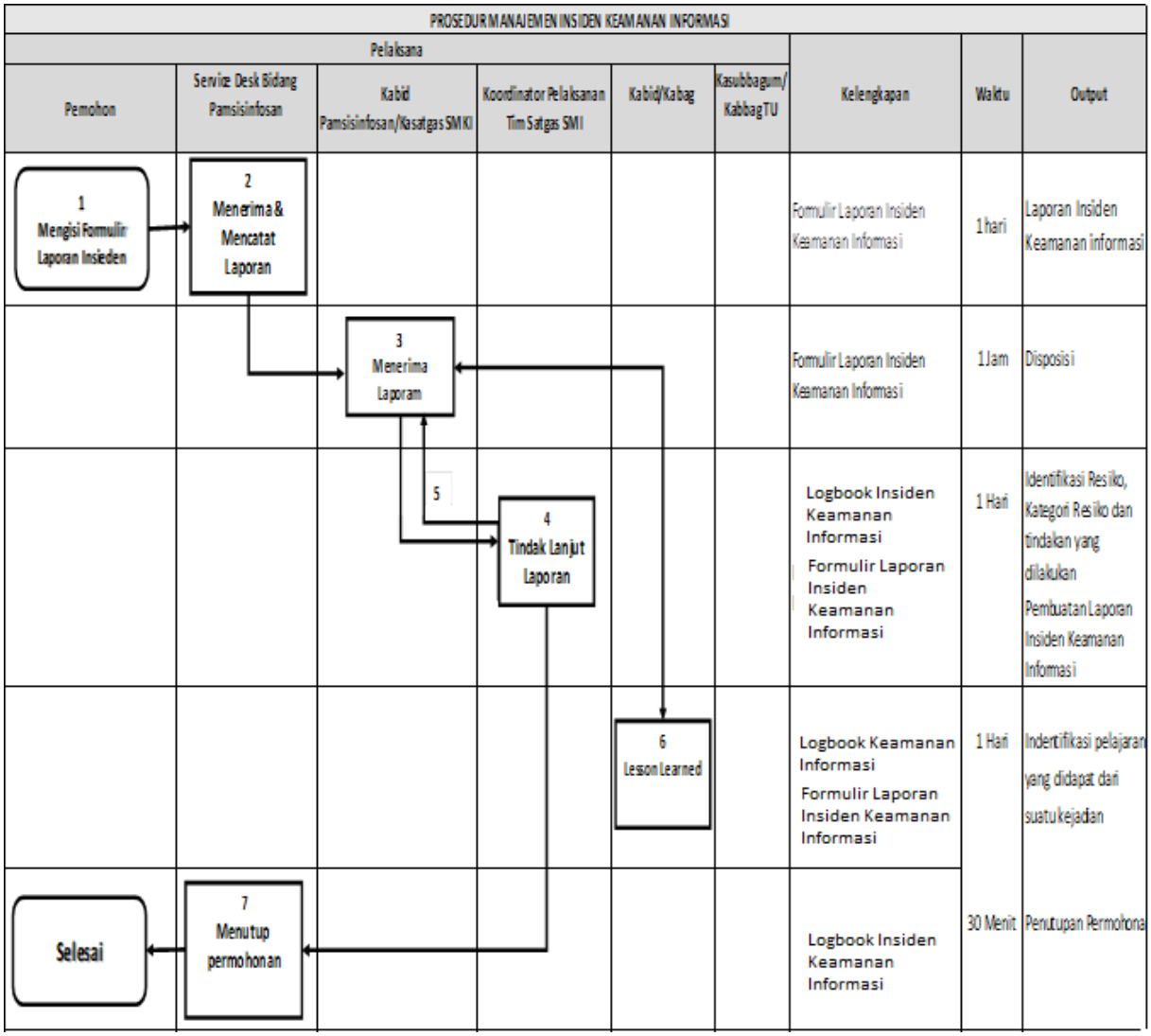
h. Tindakan yang perlu dilakukan terkait Insiden baik berupa temporary ataupun recovery dituangkan dalam *Business Continuity Plan*.

BAB IV
PROSEDUR DAN TANGGUNG JAWAB

4. Prosedur dan tanggung jawab

a. Pelaporan kelemahan dan penanganan serta tindak lanjut pelaporam gangguan insiden keamanan informasi.

Tabel 1. *Flowchart* prosedur manajemen insiden keamanan informasi



1) Uraian kegiatan

a) Pemohon atau pengguna melaporkan kelemahan atau gangguan dan insiden keamanan informasi pemohon atau pengguna menyerahkan form laporan insiden keamanan informasi beserta persyaratannya ke service desk Bidang Pamsisinfosan .

b) *Service desk* Bidang Pamsisinfosan menerima laporan dan melakukan pencatatan *Service desk* Bidang Pamsisinfosan melakukan evaluasi dan eskalasi laporan ke Kepala Bidang Pamsisinfosan atau Ketua Tim Satgas SMKI.

c) Kepala Bidang Pamsisinfosan atau Ketua Tim Satgas SMKI menerima laporan kelemahan/ gangguan dan insiden keamanan informasi

d) Kepala Bidang Pamsisinfosan atau Ketua Tim Satgas SMKI menugaskan Koordinator Pelaksana Tim Satgas SMKI untuk melakukan *follow up*/ Tindak Lanjut.

e) Koordinator Pelaksana Tim Satgas SMKI melakukan evaluasi laporan melalui identifikasi resiko *(risk assessment)*, katagori insiden dan tindakan yang dilakukan

(1) Koordinator Pelaksana Tim Satgas SMKI melakukan pembentukan dan koordinasi sumberdaya untuk melakukan penanganan.

(2) Koordinator Pelaksana Tim Satgas SMKI beserta tim melakukan penanganan dan tindakan.

(3) Koordinator Pelaksana Tim Satgas SMKI beserta tim selesai melakukan penanganan dan membuat laporan dan status untuk dikirim kepada Ketua Tim Satgas SMKI

f) Ketua Tim Satgas SMKI dan Kepala Bidang/Bagian beserta tim melakukan aktifitas identifikasi pelajaran yang didapat dari sebuah kejadian (*lesson learned)*.

g) *Service Desk* Bidang Pamsisinfosan menyampaikan kepada pemohon dan menutup permohonan

b. Pengumpulan bukti setelah gangguan insiden keamanan informasi
Tabel 2. *Flowchart* prosedur manajemen keamanan informasi.

PROSEDUR MANAJEMEN INSIDEN KEAMANAN INFORMASI						
Pelaksana				Kelengkapan	Waktu	Output
Kasatgas tim SMKI	Koordinator Pelaksanan Tim Satgas SMI	Biro Hukum	Kasubbagum/Kabbag TU			
[illegible] Pengumpulan	2 Menerima penugasan dengan Evaluasi, analisis dan laporan			Disposisi Laporan Insiden Keamanan informasi	1 hari	Pengumpulan bukti Evaluasi, Analisis dan Laporam hasil analisis
	3			Laporan Hasil analisis	1 Jam	Disposisi
		4 Tindak		Disposisi Laporan Hasil analisis	1 Hari	Tindak Lanjut
			5 Evaluasi Kelayakan Laporan Selesai	Laporan Hasil analisis	1 Hari	Evaluasi Kelayakan Laporan Tindak Lanjut secara Hukum

1) Uraian kegiatan

a) Ketua Tim Satgas SMKI menugaskan Koordinator Pelaksana atau Tim keamanan informasi melakukan pengumpulan bukti setelah insiden keamanan informasi.

b) Koordinator Pelaksana Tim Satgas SMKI mempersiapkan sumber daya dan koordinasi dengan pihak – pihak terkait.

(1) Koordinator Pelaksana Tim Satgas SMKI melakukan koleksi media.

(2) Koordinator Pelaksana Tim Satgas SMKI melakukan evaluasi data dari media yang sudah dikoleksi.

(3) Koordinator Pelaksana Tim Satgas SMKI melakukan analisis informasi dari data-data yang dihasilkan evaluasi

(4) Koordinator Pelaksana Tim Satgas SMKI mengeluarkan laporan hasil analisis

c) Koordinator Pelaksana Tim Satgas SMKI menyampaikan laporan hasil analisis kepada Ketua Tim Satgas SMKI.

d) Ketua Tim Satgas SMKI melakukan evaluasi laporan hasil analisis pengumpulan bukti setelah insiden keamanan informasi dan menyampaikan kepada biro hukum untuk ditindaklanjuti.

e) Jika diperlukan, Kepala Bagian Tata Usaha/Kasubag Umum melakukan evaluasi kelayakan laporan untuk kemudian menindaklanjuti secara hukum.

BAB V
DOKUMEN PENDUKUNG

5 Dokumen Pendukung

a. Prosedur Registrasi Asset, Penilaian Resiko, Dan Tindak Lanjut Nomor : SOP/18/VIII/2022/PUSDATIN.

b. Prosedur Penanganan Insiden Keamanan Informasi Nomor : SOP/ 20/VIII/2022/PUSDATIN.

c. Prosedur Manajemen Keberlanjutan Bisnis Nomor : SOP/21/VIII/ 2022/PUSDATIN.

BAB VI
REKAMAN PENDUKUNG

6 Rekaman Pendukung

a. Formulir Laporan Insiden Keamanan Informasi Nomor : LI/20A/ VIII/2022/PUSDATIN.

b. Formulir Logbook Insiden Keamanan Informasi Nomor : LI/20B/ VIII/2022/PUSDATIN.

BAB VII
RUJUKAN

7 Rujukan

a. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Klausul 8 *Operation.*

b. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Klausul 8.1 *Operational Planning And Control.*

c. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16 *Information Security Incident Management.*

d. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1 *Management Of Information Security Incidents And Improvements.*

e. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.1 *Responsibilities And Procedures.*

f. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.2 *Reporting Information Security Events.*

g. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.3 *Reporting Information Security Weaknesses.*

h. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.4 *Assessment Of And Decision On Information Security Events.*

i. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.5 *Response To Information Security Incidents.*

j. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.6 *Learning From Information Security Incidents.*

k. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.16.1.7 *Collection Of Evidence.*

BAB VIII
PENUTUP

8 Penutup

a. Demikian SOP Penanganan Insiden Informasi ini di buat, sebagai acuan dalam pengamanan informasi di Pusdatin.

b. Pedoman ini berlaku sejak di tandatangani dan ketentuan yang belum tercantum dalam pedoman ini akan diatur lebih lanjut dengan memperhatikan perkembangan Sistem Manajemen Keamanan Informasi.

c. Dokumen asli dari prosedur ini dipelihara dan dikendalikan oleh dokumen kontrol di Bidang Pamsisinfosan Pusdatin Kemhan RI.

d. Penggunaan dokumen asli ataupun dokumen salinan harus mengikuti aturan yang tertulis pada Dokumen Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN.

Dikeluarkan di Jakarta
Pada tanggal Agustus 2022

Kepala Pusat Data dan Informasi,

Rionardo
Brigadir Jenderal TNI

Lampiran

a. Formulir Laporan Insiden Keamanan Informasi Nomor : LI/20A/VIII/ 2022/PUSDATIN.

b. Formulir Log Book Insiden Keamanan Informasi Nomor : LI/20B/VIII/ 2022/PUSDATIN.

	KEMENTERIAN PERTAHANAN RI PUSAT DATA DAN INFORMASI	No. Dok	LI/20A/VIII/2022/PUSDATIN
		No. Rev	00
	LAPORAN INSIDEN KEAMANAN INFORMASI	Tgl	Agustus 2022
		Hal	

No. Laporan Insiden Keamanan Informasi: .....

Tujuan Pelaporan:

☐ Kelemahan (*Vulnerability*) ☐ Insiden

☐ Simulasi Kelemahan ☐ Simulasi Insiden

Petunjuk :

1. *Isilah semua data secara lengkap*
2. *Pelapor mengisi kolom A dan B secara jelas*
3. *Kirim Formulir ke Pamsisinfosan untuk di proses*
4. *Koordinator Tim Satgas dan Tim mengisi kolom C dan D sebegai tindak lanjut hasil pelaporan.*

A. Data pemohon

Nama Lengkap :

NRP/NIP/NIK :

Bagian/Bidang :

B. Uraian insiden / kelemahan sistem it

Waktu dan Tanggal Insiden :

Lokasi Insiden :

Jenis Insiden / Kelemahan :

Impact :

Pemberi Pernyataan / Pemohon

Nama :

Tanggal :

C. Tindak lanjut pelaporan (investigasi MR & tim)

Permasalahan perlu ditindaklanjuti untuk *investigasi awal*
☐ Ya ☐ Tidak
Alasan (jika ada) :

Tim Perbaikan- jika diperlukan (*atau lihat Business Continuity Team atau Tim Insiden SMKI*)

Lokasi *Emergency Operation Centre* atau *Crisis Centre*- jika diperlukan

Hasil Investigasi Masalah : (Nama & Tanggal :)

Hasil Tindakan Perbaikan (*Corrective Actions*) :
(Nama & Tanggal :)

D. Aktivasi *business continuity plan*

Permasalahan perlu ditindaklanjuti dengan Aktivasi
Business Continuity Plan

☐ Ya ☐ Tidak
Alasan (jika ada) :

Business Continuity Team atau Tim Insiden SMKI

Lokasi *Emergency Operation Centre* atau *Crisis Centre*

Hasil Investigasi Masalah :
(Nama & Tanggal :)

Hasil Tindakan Perbaikan (*Corrective Actions*) :
(Nama & Tanggal :)

Membutuhkan Biaya Pemulihan (Jika ada) :

Rincian Perbaikan :
Besarnya Biaya :

Analisis Akar Penyebab Masalah :
(Nama & Tanggal :)

Tindakan Pencegahan (*Preventive Actions*) :
(Nama & Tanggal :)

E. Status insiden / kelemahan sistem it

Setelah melakukan penelusuran terhadap permasalahan dan melakukan analisa, dengan ini saya
menyatakan bahwa insiden / kelemahan sistem statusnya adalah :

☐ *Closed* ☐ *Opened*

Alasan (jika ada) :

Tanda Tangan Koordinator Tim Satgas SMKI

Nama :
Tanggal :

Tanda Tangan Ketua Tim Satgas SMKI

Nama :
Tanggal :

	KEMENTERIAN PERTAHANAN RI PUSAT DATA DAN INFORMASI	No. Dok	: LI/20B/VIII/2022/PUSDATIN
		No. Rev	: 00
	***LOGBOOK* INSIDEN KEAMANAN INFORMASI**	Tgl	: Agustus 2022
		Hal	: 1

No	Nomor Laporan Insiden	Tanggal Laporan	Penanggung jawab	Permasalahan	Keterangan
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					