STANDAR OPERASIONAL PROSEDUR
NOMOR: 5 TAHUN 2023
PENANGANAN INSIDEN SIBER DI LINGKUNGAN BADAN PENGAWAS TENAGA NUKLIR

BADAN PENGAWAS TENAGA NUKLIR

Jl. Gajah Mada No.8 Jakarta Pusat 10120
Telepon: (+62-21) 6385 826970; 630 2164
Homepage: www.bapeten.go.id, E-mail: info@bapeten.go.id

LEMBAR PERSETUJUAN

No.	Nama	Jabatan	Tanda Tangan	Tanggal
DISIAPKAN OLEH:				
1	Achmad Bussamah, ST, MKKK	Kepala Biro Perencanaan, Informasi dan Keuangan		3/10/2023
2	Esturini Fitriyanti, S. Kom	Koordinator Kelompok Fungsi Data dan Informasi		3/10/2023
3	Harry Susanto, S. Kom., M. Eng	Pranata Komputer Ahli Muda		3/10/2023
DIPERIKSA OLEH:				
1	Ir. Dedik Eko Sumargo	Kepala Biro Organisasi dan Umum		25/10/2023
2	Eko Legowo, SE	Koordinator Kelompok Fungsi Organisasi dan Tata Laksana		23/10/2023
3	Yoga Gunara Aidid, S. Kom	Sub Koordinator kelompok Fungsi Tata Laksana		23/10/2023
4	Muhammad Andiyaksa	Analis Tata Laksana		23/10/2023

DISAHKAN OLEH:

Nama	Jabatan	Tanda Tangan	Tanggal
Sugeng Sumbarjo	Sekretaris Utama	Ditandatangani secara elektronik oleh: **Sekretaris Utama** **Sugeng Sumbarjo**	26/10/2023

LEMBAR DISTRIBUSI

Salinan SOP ini didistribusikan secara elektronik kepada seluruh pegawai di lingkungan BAPETEN.

DAFTAR ISI

1. TUJUAN

Standar operasional prosedur ini menetapkan tata cara penanganan insiden siber untuk menjaga keamanan infromasi yang dimiliki oleh Badan Pengawas Tenaga Nuklir (BAPETEN) dengan melakukan tindakan pendeteksian, penahanan, penghapusan konten, dan pemulihan untuk menjamin ketersediaan, keutuhan dan kerahasiaan setiap asset informasi yang dimiliki oleh BAPETEN

2. RUANG LINGKUP

Ruang lingkup standar operasional prosedur meliputi tata cara penanganan insiden siber yang berlaku di lingkungan BAPETEN

3. DEFINISI

3.1 BAPETEN CSIRT adalah anggota yang memiliki susunan tim tanggap insiden siber yang terdiri dari ketua, sekretaris, koordinator BAPETEN CSIRTdan anggota lainnya yang tertuang dalam Keputusan Kepala Badan Pengawas Tenaga Nuklir Republik Indonesia Nomor 0301 Tahun 2023 Tentang Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*) Badan Pengawas Tenaga Nuklir yang yang bertanggung jawab untuk menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber dilingkungan BAPETEN;

3.2 Log adalah file yang dihasilkan perangkat lunak yang berisi informasi mengenai operasi, aktivitas, dan pola penggunaan aplikasi, server, atau perangkat lainnya yang dapat digunakan sebagai untuk menganalisa status pada sebuah sistem TIK seperti *log-event, log-access*, dsb;

3.3 Aplikasi *Ticketing* adalah aplikasi *ticketing* yang digunakan untuk melaporkan insiden siber yang dialami oleh user, mengacu kepada kategori insiden yang nantinya akan di tindaklanjuti dan di respons oleh tim dalam hal ini BAPETEN;

3.4 Pemulihan (*Recovery*) adalah suatu tindakan yang dilakukan untuk proses pemulihan agar perangkat atau sistem IT dapat pulih seperti sedia kala dan berjalan dengan normal;

3.5 Penahanan (*Containment*) adalah membatasi kerusakan dan mencegah terjadinya kerusakan lebih lanjut;

3.6 Pemberantasan (*Eradication*) adalah pemindahan dan pemulihan dari sistem yang terkena dampak;

4. IDENTITAS

BADAN PENGAWAS TENAGA NUKLIR	**NOMOR SOP**	:	5 Tahun 2023
	TGL. PEMBUATAN	:	3 Oktober 2023
	TGL. REVISI	:	-
	TGL. EFEKTIF	:	26 Oktober 2023
	NAMA SOP	:	Penanganan Insiden Siber di Lingkungan Badan Pengawas Tenaga Nuklir
	REVISI KE	:	0
	JENIS SOP	:	Prosedur Administrasi

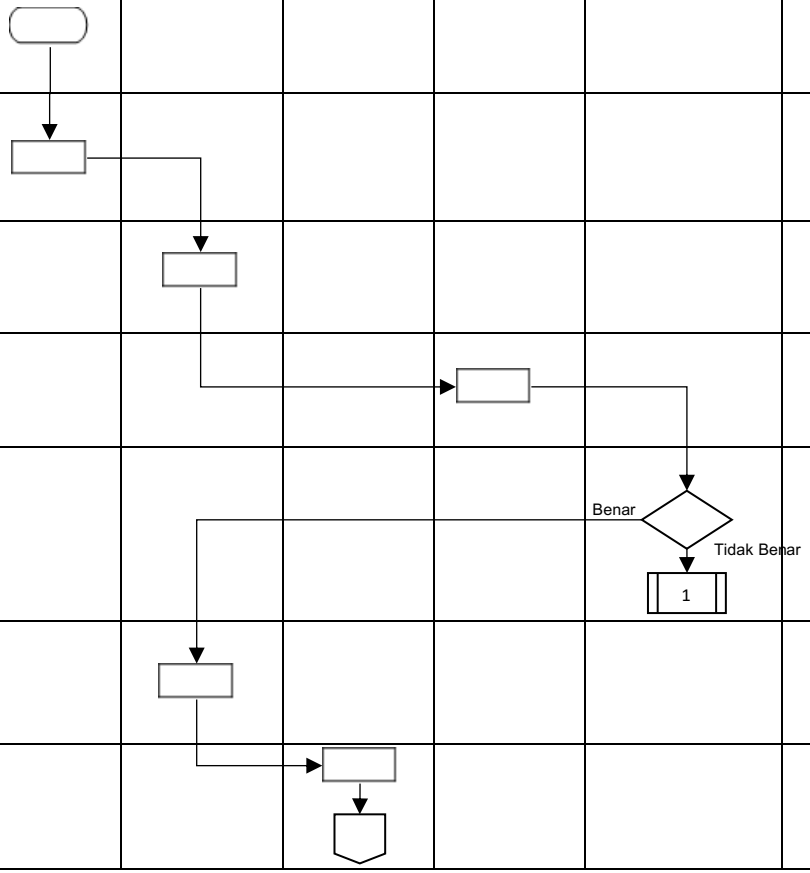
ACUAN	**KUALIFIKASI PELAKSANA**
1. Peraturan Kepala BAPETEN Nomor 14 Tahun 2014 Tentang Sistem Manajemen Badan Pengawas Tenaga Nuklir. 2. Peraturan Kepala BAPETEN Nomor 1 Tahun 2018 Tentang Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Badan Pengawas Tenaga Nuklir. 3. Peraturan Badan Pengawas Tenaga Nuklir Republik Indonesia Nomor 8 Tahun 2020 Tentang Sistem Manajemen Keamanan Informasi Di Lingkungan Badan Pengawas Tenaga Nuklir; 4. Peraturan BAPETEN Nomor 6 tahun 2021 tentang Tata Naskah Dinas dan Klasifikasi Arsip Badan Pengawas Tenaga Nuklir;	1. Memiliki pengetahuan yang memadai dalam pengelolaan tata kelola Teknologi Informasi dan Komunikasi (TIK) di lingkungan BAPETEN; 2. Memiliki pemahaman penanganan insiden siber seperti pemeriksaan log-event, access log, dsb;

KETERKAITAN	PERALATAN/PERLENGKAPAN
1. SOP Keadaan Darurat Sistem Elektronik Balis Perizinan dan Balis Pekerja	1. Personal Komputer/*Notebook* 2. Aplikasi Pengetikan*;* 3. Akses Jaringan Intranet dan Internet; 4. Mesin Pencetak (*printer*).
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Apabila SOP ini tidak dilaksanakan dengan baik maka penanganan insiden siber di Badan di lingkungan Badan Pengawas Tenaga Nuklir akan terhambat.	**1.** LAMPIRAN 1. Format Laporan Insiden Siber

5. ALUR PROSE

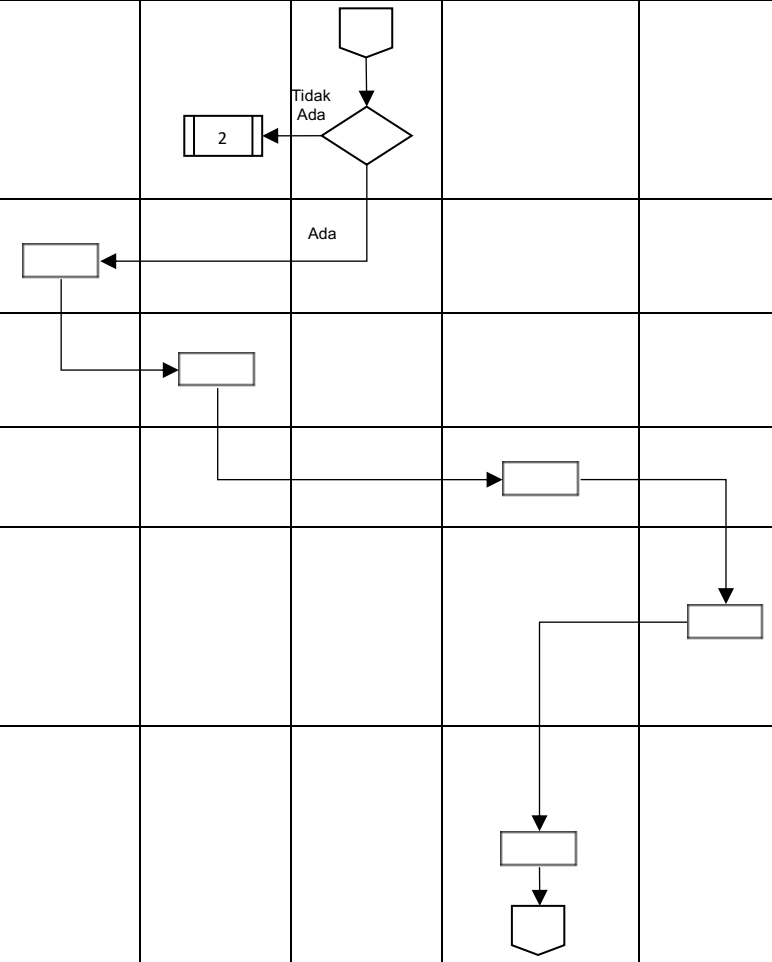
5.1 Proses Penangan Insiden Siber

No.	Kegiatan	Pelaksana						Mutu Baku			Ket.
		Kepala Unit Kerja	Ketua CSIRT (Ka. BPIK)	Koordinator CSIRT	Tim CSIRT (BAPETEN)	Tim Teknis Utama CSIRT	Pihak Eksternal (CSIRT Nasional)	Kelengkapan	Waktu	Output	
1.	Menyampaikan laporan terjadinya insiden siber									Laporan	Laporan disampaikan melalu aplikasi
2.	Menunjuk anggota BAPETEN CSIRT untuk melakukan penanganan sesuai dengan tugasnya							Informasi pelaporan insiden, Bukti insiden	30 Menit	Ticket pelaporan	Informasi pelaporan insiden, Bukti insiden
3.	Menindaklanjuti tiket pelaporan yang masuk pada aplikasi ticket							Ticket Pelaporan	30 menit	Ticket Pelaporan dan Informasi Laporan Insiden	Ticket Pelaporan
4.	Memeriksa gangguan pada laporan ticket							Ticket Pelaporan dan Informasi Laporan Insiden	2 Jam	Jurnal insiden keamanan	Ticket Pelaporan dan Informasi Laporan Insiden
5.	Mengevaluasi kebenaran gangguan insiden siber : • Jika benar, maka lanjut ke proses selanjutnya • Jika tidak benar maka lanjut ke proses akhir							Jurnal insiden keamanan	1 jam	Hasil evaluasi	Lewat aplikasi dengan perubahan status
6.	Mengirimkan pemberitahuan kepada Pemilik / Penanggung-Jawab Aset tentang adanya insiden siber kepada Ketua CSIRT dan unit kerja/pemohon							Hasil evaluasi	2 Minggu	Hasil pemberitahuan	
7.	Menganalisis insiden keamanan yang dilaporkan dengan menentukan prioritas dan rencana penanganan							Hasil pemberitahuan	1 Jam	Log gangguan insiden siber	



No.	Kegiatan	Pelaksana						Mutu Baku			Ket.
		Kepala Unit Kerja	Ketua CSIRT (Ka. BPIK)	Koordinator CSIRT	Tim CSIRT (BAPETEN)	Tim Teknis Utama CSIRT	Pihak Eksternal (CSIRT Nasional)	Kelengkapan	Waktu	Output	
8.	Menunjuk anggota BAPETEN CSIRT untuk melakukan penanganan sesuai dengan tugasnya							Log gangguan insiden siber	30 menit	Disposisi	
9.	Penanganan secara teknis sesuai dengan identifikasi dan mitigasi							Disposisi	1 Hari	Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dll	Meliputi tindakan - Penahanan (containment); - Penghapusan konten (eradication); - Pemulihan
10.	Terjadi kendala dalam penanganan secara teknis (1): • Jika ada kendala, maka dilanjutkan ke proses nomor 11 • Jika tidak ada kendala, maka dilanjutkan ke proses nomor 13					Ada Tidak Ada		Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dll	1 Jam	Laporan kendala penanganan	
11.	Melaporkan kendala dalam penanganan insiden siber							Laporan kendala penanganan	30 Menit	Laporan dan Log penanganan insiden siber	Lewat aplikasi dengan perubahan status
12.	Mengevaluasi kebutuhan penanganan insiden siber							Laporan dan Log penanganan insiden siber	1 Jam	Disposisi dan Arahan	
13.	Penanganan secara teknis oleh Tim BAPETEN CSIRT			2				Disposisi dan Arahan	1 Hari	Log penanganan insiden siber berupa laporan hasil penanganan, recovery, dll oleh tim CSIRT	Meliputi tindakan - Penahanan (containment); - Penghapusan konten(eradication); - Pemulihan

No.	Kegiatan	Pelaksana						Mutu Baku			Ket.
		Kepala Unit Kerja	Ketua CSIRT (Ka. BPIK)	Koordinator CSIRT	Tim CSIRT (BAPETEN)	Tim Teknis Utama CSIRT	Pihak Eksternal (CSIRT Nasional)	Kelengkapan	Waktu	Output	
14.	Terjadi kendala dalam penanganan secara teknis (2): • Jika ada kendala, maka lanut ke proses nomor 15 • Jika tidak ada kendala, maka kembali ke proses nomor 13							Log penanganan insiden siber berupa laporan hasil penanganan, recovery, dll oleh tim CSIRT	1 Jam	Laporan kendala penanganan	
15.	Melaksanakan langkah-langkah yang diperlukan untuk mendapat bantuan eksternal.							Laporan kendala penanganan	2 Jam	Surat dan Dokumen Laporan penanganan	
16.	Menghubungi pihak eksternal untuk mendapatkan bantuan penanganan							Surat dan Dokumen Laporan penanganan	30 Menit	Respon pihak eksternal	
17.	Menunjuk anggota tim teknis BAPETEN CSIRT untuk melakukan penanganan dengan bantuan pihak luar							Respon pihak eksternal	1 Jam	Disposisi	
18.	Penanganan secara teknis oleh Pihak Eksternal							Disposisi	2 Hari	Log penanganan insiden siber berupa laporan hasil penanganan, recovery, dll oleh pihak eksternal	Meliputi tindakan - Penahanan (containment); - Penghapusan konten (eradication); - Pemulihan
19.	Melakukan pencatatan detail penanganan dan pengumpuan dokumentasi							Log penanganan insiden siber berupa laporan hasil penanganan, recovery, dll oleh pihak eksternal	2 Jam	Dokumentasi penanganan teknis	



No.	Kegiatan	Pelaksana						Mutu Baku			Ket.
		Kepala Unit Kerja	Ketua CSIRT (Ka. BPIK)	Koordinator CSIRT	Tim CSIRT (BAPETEN)	Tim Teknis Utama CSIRT	Pihak Eksternal (CSIRT Nasional)	Kelengkapan	Waktu	Output	
20.	Memeriksa kesesuaian penyelesaian insiden keamanan dan semua rincian insiden, tindakan-tindakan yang dilakukan, serta bukti-bukti insiden telah dicatat dan disimpan sesuai dengan ketentuan yang berlaku							Dokumentasi penanganan teknis	1 Jam	Laporan teknis penyelesaian penanganan insiden	
21.	Melaporkan penyelesaian teknis penanganan insiden							Laporan teknis penyelesaian penanganan insiden	30 Menit	Laporan akhir penanganan insiden	
22.	Penutupan ticket pelaporan insiden siber					1		Laporan akhir penanganan insiden	30 Menit	Dokumen penutupan ticket, laporan akhir penanganan insiden	

LAMPIRAN

LAMPIRAN 1. Format Laporan Insiden Siber

	BAPETEN CSIRT
	LAPORAN INSIDEN SIBER
A. DATA PELAPOR	
Nama Lengkap	:
Nama Satuan Kerja	:
Alamat Instansi	:
No. Handphone	:
Email	:
B. URAIAN INSIDEN / KELEMAHAN SISTEM IT	
Waktu/Tanggal Insiden	:
Lokasi Insiden	:
Jenis Insiden	: (Phising, Deface, Pembajakan Akun, Akses Ilegal, Spam, Hoax, DDoS, Malware, Virus, Lainnya……) *) ***) Pilih**
Deskripsi Insiden (URL, IP, Gambar, Log)	
Dampak Insiden	
Penahanan (*containment*)	
Penghapusan konten (*eradication*)	
Pemulihan (*Recovery*)	

……., …….20

--ttd--

(Nama Penyusun)