STANDAR OPERASIONAL PROSEDUR

PENGELOLAAN GANGGUAN DAN MANAJEMEN INSIDEN

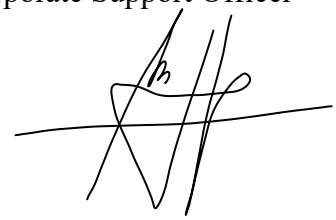
2026

Gedung AirNav Indonesia.
Jl. Ir. H. Juanda, Tangerang , 15121, Banten – Indonesia

<table>
<tr><td rowspan="5"> 
AirNav Indonesia

PERUM LEMBAGA
PENYELENGGARA PELAYANAN NAVIGASI PENERBANGAN INDONESIA
AIRNAV INDONESIA</td><td>NOMOR SOP</td><td>SOP.001/SS/00/LPPNPI/ KMP12.12.01/I/2026</td></tr>
<tr><td>TANGAL PENGESAHAN</td><td>20 Januari 2026</td></tr>
<tr><td>TANGGAL REVISI</td><td></td></tr>
<tr><td>DISETUJUI OLEH</td><td>EXECUTIVE VICE PRESIDENT STANDARD AND SECURITY</td></tr>
<tr><td>NAMA SOP</td><td>SOP PENGELOLAAN GANGGUAN DAN MANAJEMEN INSIDEN</td></tr>
<tr><td>DESKRIPSI</td><td colspan="2">TUJUAN</td></tr>
<tr><td>SOP Pengelolaan dan Manajemen Insiden ini digunakan untuk penanganan jika terjadi gangguan (insiden/permasalahan sangat penting berdasarkan pengklasifikasian (ketegorisasi dan penentuan skala prioritas) dan dukungan awal bagi karyawan pada saat terjadi insiden</td><td colspan="2">1. Sebagai kerangka kerja yang sistematis dan terstruktur guna mendeteksi, merespons, ,memulihkan dan mengurangi dampak insiden keamanan siber secara efektif dan efisien.
2. Sebagai jaminan bahwa setiap insiden dilaporkan, ditindaklanjuti, dievaluasi untuk meminimalkan dampak dan mencegah terulangnya insiden</td></tr>
<tr><td>DASAR HUKUM</td><td colspan="2">KUALIFIKASI PELAKSANAAN</td></tr>
<tr><td>1. Undang-Undang Nomor 1 Tahun 2009 Tentang Penerbangan ;
2. Undang-Undang Nomor 11 tahun 2008 tentang ITE serta perubahannya (UU No.19/2016 & UU No.1/20240;
3. PP No.71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ;
4. Perpres Nomor 82 tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital;</td><td colspan="2">1. Personel memiliki kemampuan mengoperasikan server.
2. Personel memiliki kemampuan mengoperasikan tools penanggulangan pemulihan insiden keamanan siber
3. Personel memiliki kemampuan membaca topologi jaringan</td></tr>
</table>

5. Keputusan Direksi Perusahaan Umum (Perum) Lembaga Penyelenggara Pelayanan Navigasi Penerbangan Indonesia Nomor : KEP.6028/U/LPPNPI/TIK.02.01/XII/2025Tentang Tim Tanggap Insiden Siber *(Computer Security Incident Response Team)* ; 6. Perusahaan Umum (Perum) Lembaga Penyelenggara Pelayanan Navigasi Penerbangan Indonesia Nomor : PER.008/LPPNPI/II/2023 Tentang Sistem Manajemen Keamanan Informasi ; 7. Nota Kesepahaman Antara Perum LPPNPI dengan Badan Siber dan Sandi Negara Republik Indonesia Tentang Perlindungan Informasi dan Transaksi Elektronik Nomor MOU.003/U/00/LPPNPI/KMP.13/II/2023 8. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber.	4. Personel memiliki kemampuan membaca log server 5. Personel memiliki kemampuan analis penyebab insiden siber 6. Memiliki kemampuan dalam membaca diagram alur/ *flowchart*.
KETERKAITAN	PERLENGKAPAN
1. SOP Penanganan Insiden Serangan SQL Injection 2. SOP Penanganan Insiden Ransomware 3. SOP Penanganan Insiden Serangan Phising 4. SOP Penanganan Insiden Web Defacement 5. SOP Penanganan Insiden Malware 6. SOP Penanganan Insiden Serangan DDoS	1. Komputer 2. Server 3. Tools penanggulangan insiden dan pemulihan sistem 4. Jaringan Internet 5. Printer
PERINGATAN	PENCATATAN dan PENDATAAN
1. Apabila prosedur ini dilaksanakan, server dan aplikasi (IT dan OT) akan terpantau dan dapat ditindaklanjuti secara cepat ketika terjadi insiden maupun serangan siber ;	1. Laporan Insiden Siber, berasal dari pihak internal maupun pihak (eksternal) baik itu Pihak Ketiga Perusahaan yang berkontrak dengan Perum LPPNPI.

2. Apabila prosedur ini tidak dilaksanakan, server dan aplikasi (IT dan OT) yang menjadi sasaran insiden maupun serangan siber tidak dapat segera diperbaiki dan bisa menjadi celah keamanan yang mengancam aplikasi-aplikasi lain yang berada dalam satu server danatau jaringan dengan aplikasi tersebut ; 3. Apabila prosedur ini dilaksanakan oleh pihak-pihak atau individu yang tidak memiliki kompetensi yang disebutkan, proses penanganan insiden siber tidak akan berjalan dengan baik, karena aspek-aspek yang mungkin harus dilaporkan dianalisis dan diperbaharui tidak terindentifikasi secara lengkap.	2. Laporan Analisis Penyebab Insiden Siber serta Rekomendasi Penanggulangan Insiden Siber 3. Laporan Akhir
Kolom Tanda Tangan	
Dibuat Oleh,	
Corporate Support Officer  **BUYUNG PRASTIYONO**	Staff Administrasi  **MIFTACHULHUDA**
Diperiksa Oleh, Vice President Of Cyber Security Assurance  **DEDY KRISTANTO**	

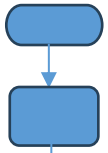
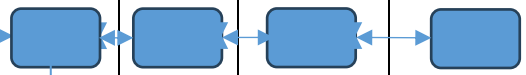
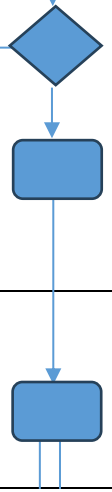
Disetujui Oleh,

Executive Vice President Of

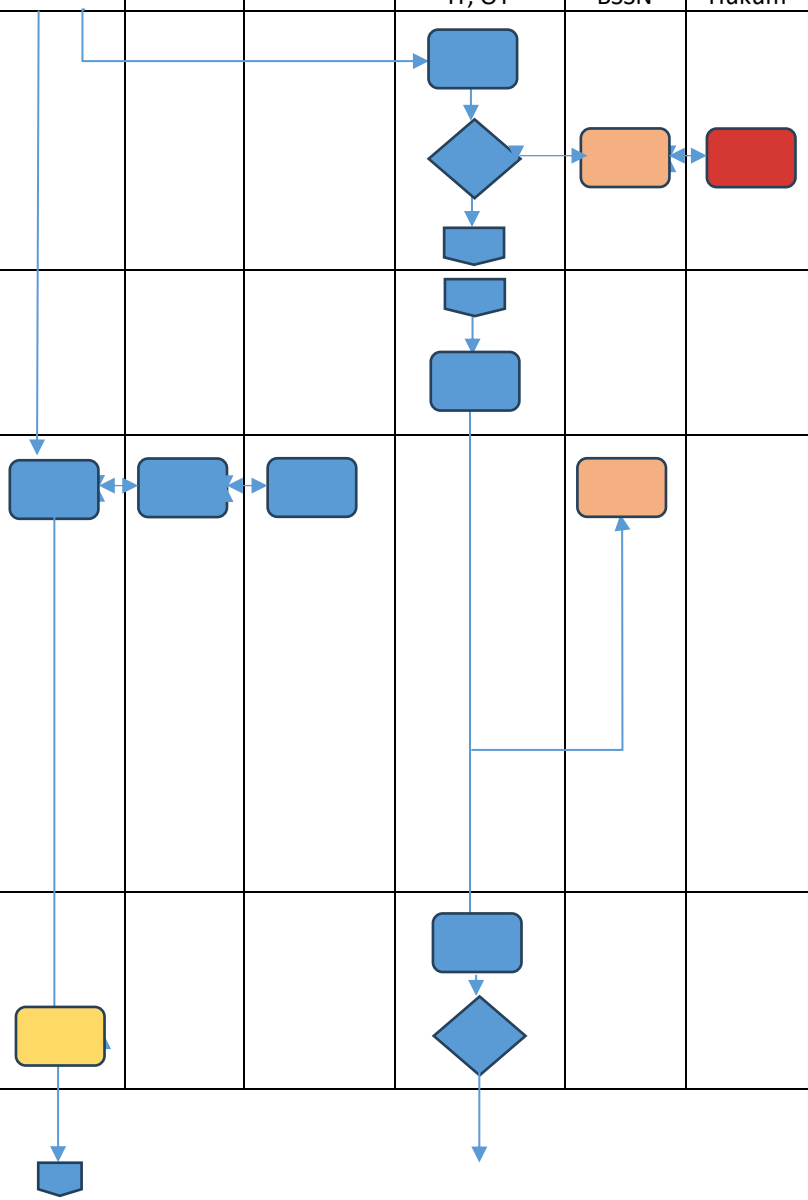
Standard and Security

VERANTY

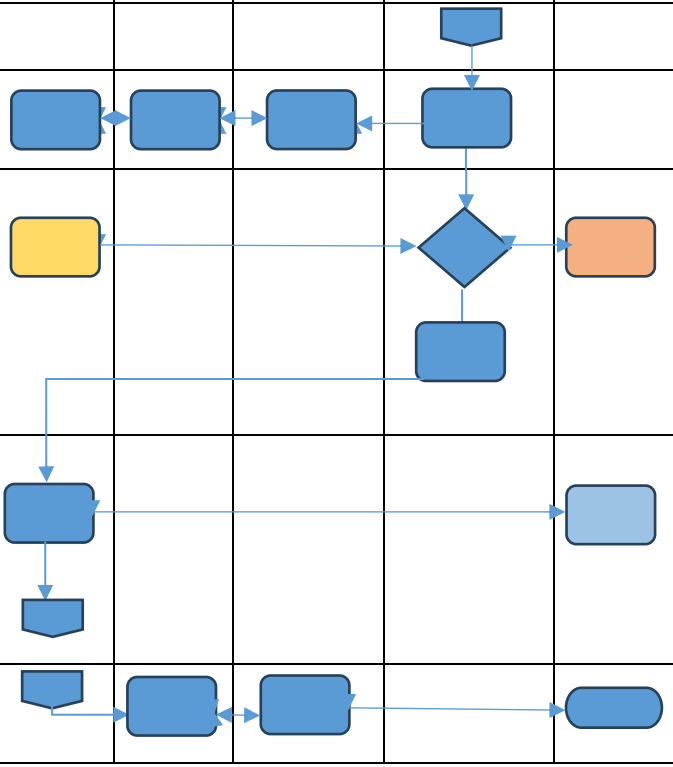
FLOWCHART PENGELOLAAN GANGGUAN DAN MANAJEMEN INSIDEN DI PERUM LPPNPI

No	Uraian Kegiatan	AirNav-CSIRT Pelaksana *							Mutu Baku			Keterangan
		Pelapor	PoC	Ketua	Sekretaris	Koordinator IT, OT	DKP, BSSN	Penegak Hukum	Persyaratan/ Kelengkapan	Waktu	Output	
1	Menerima laporan insiden siber								Komputer/ Email/ Message (WA)/ Telephone	5 menit	Laporan Awal Insiden Siber	Laporan dapat berasal dari pihak luar (eksternal) maupuan dari internal : tim insiden management cabang/pengembang / SOC/anggota (surat/email)
2	Meneruskan laporan insiden siber untuk langkah tindak lanjut								Laporan Awal Insiden Siber	5 menit	Form Aduan Insiden Siber	Menerima laporan insiden oleh Tim AirNav-CSIRT dan menentukan rencana tindak lanjut (Apakah kategori Insiden TI atau Non TI)
3	AirNav-CSIRT memverifikasi laporan insiden siber								Form Aduan Insiden Siber	5 menit	Laporan Terverifikasi **Valid**, segera ditindaklanjuti **Tidak Valid** tidak ditindaklanjuti	Verifikasi laporan insiden terkait : Identitas pelapor, Jenis insiden siber, Lokasi, Sistem log
4	Melakukan Analisa Insiden								Laporan Insiden Siber Valid	10 menit	Laporan Analisis Awal	Analisa insiden, untuk menentukan kategori insiden siber dan melanjutkan penanganan sesuai dengan SOP

No	Uraian Kegiatan	AirNav-CSIRT Pelaksana *							Mutu Baku			Keterangan
		Pelapor	PoC	Ketua	Sekretaris	Koordinator IT, OT	DKP, BSSN	Penegak Hukum	Persyaratan/ Kelengkapan	Waktu	Output	
5	Menyusun strategi mitigasi terhadap insiden siber sesuai SOP yang telah disusun								Laporan Analisis Awal	Maks. 23 jam	SOP Penanganan Insiden Siber dan tim teknis	Jika Insiden Siber tidak dapat ditangani akan melibatkan DKP dan BSSN untuk penanganan insiden siber. Menyesuaikan tingkat kritikalitas aplikasi: Rendah, Sedang, Kritis ***Rendah** : maksimal 24 jam, perkiraan waktu yang diperlukan untuk menyelesaikan insiden siber dan mampu untuk menangani. ***Sedang :** > 24 jam, harus segera meminta bantuan ***Kritis** : Langsung berkolaborasi dengan Unit terkait (Internal / eksternal)
6	Melaksanakan penanganan insiden siber sesuai strategi mitigasi yang disusun								SOP Penanganan Insiden Siber		Skenario Penanganan	
7	Menyampaikan laporan analisis dan rekomendasi insiden siber								Skenario	2 jam	Tools	
8	Melaksanakan perbaikan terhadap insiden								Tools	120 jam	Eskalasi Insiden	Eskalasi Teknis ke pengembang, pihak ketiga SOC jika insiden tidak bisa ditangani dan perlu lebih cepat



No	Uraian Kegiatan	AirNav-CSIRT Pelaksana *							Mutu Baku			Keterangan
		Pelapor	PoC	Ketua	Sekretaris	Koordinator IT, OT	DKP, BSSN	Penegak Hukum	Persyaratan/ Kelengkapan	Waktu	Output	
9	Melaporkan hasil penanganan insiden siber									24 jam	Laporan Perbaikan	Melakukan investigasi dan diagnosis
10	Memeriksa dan testing hasil perbaikan									1 minggu	Laporan Testing	Sudah Selesai / Butuh Perbaikan ulang Dengan Meminta Pihak Ketiga untuk melakukan Penetration Test / VA
11	Menginformasikan, tanggapan berupa langkah-langkah terkait penangan insiden siber yang telah dilaksanakan									2 jam	Tanggapan Laporan Siber	PoC menginformasikan ke Koordinator Hubungan Masyarakat dan Hukum tentang penanganan insiden Siber
12	Menyusun laporan penanganan insiden siber									1 – 2 Minggu	Laporan Akhir Siber	



Koordinator PoC : VP *Cyber Security Assurance*

PoC : *Cyber Security Assurance*

Ketua : *EVP of Standard and Security*

Sekretaris : *EVP of Corporate Secretary*

Koordinator IT : *EVP of Information Technology* (IT)

Subkoordinator IT : *VP of Network Operation, VP of IT Operation, VP of Enterprise Technology Planning and ITBP*

Koordinator OT : *EVP of Infrastructure Readiness* (OT)

Subkoordinator OT : *VP of Communication and Navigation Facility Readiness, VP of Surveillance and Data Processing Facility Readiness, VP of Support Management*