PEMERINTAH DAERAH ISTIMEWA YOGYAKARTA

DINAS KESEHATAN

RUMAH SAKIT JIWA GRHASIA

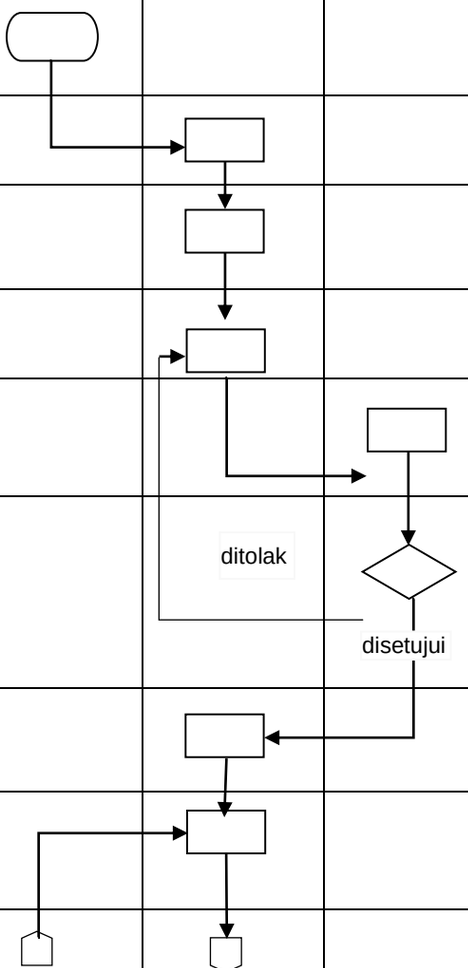
Jalan Kaliurang Km 17 Sleman Kode Pos 55582 Telepon: (0274) 895143. 895297, Faksimile: (0274)895142
Laman: grhasia.jogjaprov.go.id Surel: grhasiamentalhospital@jogjaprov.go.id

Nomor SOP	
Tanggal Pembuatan	05 Januari 2026
Tanggal Revisi	-
Tanggal Efektif	05 Januari 2026
Disahkan Oleh	DIREKTUR, dr. AKHMAD AKHADI S., M.P.H
Nama SOP	Manajemen Keamanan Informasi

Dasar Hukum	**Kualifikasi Pelaksana**
1. Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik 2. Peraturan Komisi Informasi Republik Indonesia Nomor 1 Tahun 2021 Tentang Standar Layanan Informasi Publik 3. Peraturan Menteri Dalam Negeri Nomor 52 Tahun 2011 tentang Standar Operasional Prosedur Di Lingkungan Pemerintah Provinsi Dan kabupaten/Kota 4. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi No. 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintah 5. Peraturan Daerah Daerah Istimewa Yogyakarta Nomor 4 Tahun 2021 tentang Pengelolaan Keterbukaan Informasi Publik 6. Peraturan Daerah Istimewa Daerah Istimewa Yogyakarta Nomor 1 Tahun 2022 tentang Kelembagaan Pemerintah Daerah Daerah Istimewa Yogyakarta 7. Peraturan Gubernur DIY Nomor 117 Tahun 2014 tentang Pedoman Penyusunan Standar Operasional Prosedur Penyelenggaraan Pemerintah Daerah.	1. Kemampuan manajemen insiden yang mencakup koordinasi, eskalasi insiden, dan pelaporan 2. Keterampilan komunikasi yang kuat untuk memberikan informasi kepada pemangku kepentingan dan bekerja sama dengan tim terkait saat insiden terjadi 3. Kemampuan analisis untuk menyelidiki sumber insiden dan menentukan penyebab utama, serta pemulihan dari insiden.
Keterkaitan	**Peralatan/Perlengkapan**
1. SOP Rapat 2. SOP Pengarsipan	1. Ruangan rapat internal 2. Komputer, Printer, LCD, ATK 3. Jaringan internet
Peringatan	**Pencatatan dan Pendataan**
Apabila prosedur tidak dilaksanakan dapat menghambat penyampaian informasi publik kepada masyarakat;	Disimpan sebagai dokumen standar layanan informasi dan untuk pedoman pelaksanaan kegiatan;

SOP : Manajemen Keamanan Informasi

NO	URAIAN PROSEDUR	PELAKSANA			MUTU BAKU			Keterangan
		Staff Subbagian Data dan Teknologi Informasi	Kasubbag Data dan Teknologi Informasi	KepalaBagian Program, Keuangan, Data dan Teknologi Informasi	Persyaratan/ Kelengkapan	Waktu	Output	
1	2	3	4	5	6	7	8	9
1	Melakukan monitoring dan evaluasi keamanan informasi secara rutin dan melaporkan hasil nya				1. Komputer/Laptop/ Handphone 2. Jaringan Internet	10Menit	LaporanTemuanInsiden	
2	Menerima laporan monitoring dan evaluasi keamanan informasi				1. Komputer/Laptop 2. Jaringan Internet	6 Jam	LaporanTemuanInsidensudahditerima	
3	Melakukan pencatatan ke dalam log insiden apabila ditemukan adanya insiden keamanan informasi				1. Komputer/Laptop 2. Jaringan Internet	1 Jam	LaporanPencatanInsiden	
4	Membuat dan mengajukan draft surat pemberitahuan insiden keamanan informasi				1. Komputer/Laptop 2. Jaringan Internet	4 jam	Draft suratpemberitahuaninsiden	
5	Menerima dan memeriksa draft surat pemberitahuan insiden kemanan informasi				1. Komputer/Laptop 2. Jaringan Internet	2 jam	Draft suratpemberitahuaninsidensudahdiperiksa	
6	Proses pengambilan keputusan atas draft surat pemberitahuan insiden keamanan informasi apakah disetujui atau ditolak. Jika disetujui maka surat dikirim ke tujuan dan ditunjuk PIC. Jika ditolak maka draft surat akan direvisi		ditolak	disetujui	1. Komputer/Laptop 2. Jaringan Internet	1 Jam		
7	Mengirimkan surat pemberitahuan insiden keamanan informasi kepada seluruh pihak terkait				1. Komputer/Laptop 2. Jaringan Internet	30 Menit	suratpemberitahuaninsidensudahdikirimkan	
8	Melakukan perbaikan dan mendokumentasikan proses perbaikan insiden keamanan informasi				1. Komputer/Laptop 2. Jaringan Internet 3. Tools Penanganan Insiden	3 Hari	Insidensudahditindaklanjuti	



9	Menginformasikan kepada Pelapor terkait tindakan perbaikan yang telah dilakukan.				1. Komputer/Laptop/ Handphone 2. Jaringan Internet	30 Menit	Informasitindaklanjutinsidenditerimapelapor	
10	Mengkonfirmasi tindakan perbaikan yang telah dilakukan. Jika masih ditemukan insiden keamanan informasi maka akandilakukan proses perbaikan kembali dan jika tidak ditemukan insiden keamanan informasi maka akan dibuat laporan penyelesaian insiden kemanan informasi	masihada tidakada			1. Komputer/Laptop/ Handphone 2. Jaringan Internet	4 Jam	Tindaklanjutinsidenberhasildiverifikasi oleh Pelapor	
11	Membuat laporan penyelesaian insiden keamanan informasi				1. Komputer/Laptop 2. Jaringan Internet	1 Hari	LaporanPenangananInsiden	
12	Mendokumentasikan sebagai arsip dan dokumen Bagian				1. Komputer/Laptop 2. Jaringan Internet	10 Menit	DokumenArsipLaporanPenangananInsiden	