



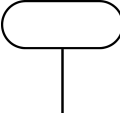
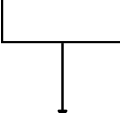
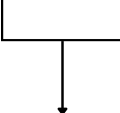
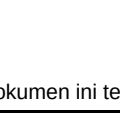
KEMENTERIAN AGAMA REPUBLIK INDONESIA
KANTOR WILAYAH KEMENTERIAN AGAMA
DAERAH ISTIMEWA YOGYAKARTA

Jl. Sukonandi No. 8 Semaki, Yogyakarta
Telepon (0274) 513492 | Faksimili (0274) 516030
Surel : kanwildiy@kemenag.go.id
Website: diy.kemenag.go.id

Nomor SOP	Kw.12.1/4763.1/OT/06/2024
Tgl Pembuatan	06 / 01 / 2024
Tgl Revisi	06 / 07 / 2026
Tgl Efektif	06 / 07 / 2026
Disahkan Oleh	Kepala Bagian Tata Usaha  H. ABD SU'UD S.Ag, M.S.I NIP. 197105031996031001

SOP KEAMANAN INFORMASI

Dasar Hukum: - Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). - Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE). - Peraturan Menteri Agama Nomor 72 Tahun 2022 tentang Organisasi dan Tata Kerja Kementerian Agama (terkait tupoksi pengelolaan TIK).	Kualifikasi Pelaksana: - Pranata Komputer - Analisis Kebijakan - Kepala Bagian Tata Usaha - Kepala Kantor
Keterkaitan: - SOP Pendokumentasian Informasi yang Dikecualikan - SOP Penetapan dan Pemutakhiran DIP	Peralatan/Perlengkapan: - Perangkat Lunak Antivirus, Firewall, dan Alat Enkripsi Data. - Server Lokal Kemenag / Fasilitas Backup Data (Storage Server). - Software Network Monitoring Tool. - Dokumen Laporan Insiden Keamanan Informasi & Log Book Akses Server.
Peringatan: Jika SOP tidak dilaksanakan, maka layanan tidak maksimal atau terhenti.	Pencatatan dan Pendataan: Disimpan sebagai data elektronik dan manual

No	Aktivitas	Pelaksana				Mutu Baku			Ket.
		Pranata Komputer	Analisis Kebijakan	Kepala Bagian Tata Usaha	Kepala Kantor	Persyaratan/Perlengkapan	Waktu	Output	
1.	Melakukan konfigurasi keamanan sistem.					Software Keamanan, Server	1 hari	Sistem yang terproteksi	—
2.	Membuat pencadangan data informasi publik dan data dikecualikan ke storage.					Harddisk External, Cloud Storage	1 hari	Salinan cadangan (backup) data	—
3.	Melakukan pemantauan lalu lintas jaringan dan mengidentifikasi potensi serangan siber.					Aplikasi Monitoring Jaringan, PC	1 hari	Log aktivitas sistem	—
4.	Menerima laporan insiden keamanan dan melakukan isolasi sistem sementara.					Form Laporan Insiden	15 menit	Sistem terisolasi	—
5.	Melakukan analisis teknis, investigasi forensik digital dan melakukan perbaikan sistem yang terinfeksi.					Software Forensic	1 hari	Penyebab insiden teridentifikasi	—
6.	Melakukan telaah kebijakan akibat insiden keamanan informasi terhadap organisasi dan publik.					Lembar Telaah Dampak	1 hari	Rekomendasi mitigasi dampak hukum	—
7.	Mengoordinasikan langkah-langkah pemulihan pasca-insiden dan memvalidasi laporan kronologi kejadian.					Draf Laporan Insiden	1 hari	Laporan final insiden tervalidasi	—

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

No	Aktivitas	Pelaksana				Mutu Baku			Ket.
		Pranata Komputer	Analisis Kebijakan	Kepala Bagian Tata Usaha	Kepala Kantor	Persyaratan/Perlengkapan	Waktu	Output	
8.	Menandatangani laporan resmi penanganan insiden dan menetapkan kebijakan peningkatan keamanan informasi yang baru.					Dokumen Laporan Resmi	1 hari	Kebijakan peningkatan keamanan disahkan	—

Seluruh tahapan kegiatan ini dilaksanakan dengan standar pelayanan prima dan profesional dalam rangka mewujudkan ZI-WBK dan WBBM, bebas dari korupsi dan gratifikasi.