STANDAR OPERASIONAL PROSEDUR LAYANAN TEKNOLOGI INFORMASI (E-Journal)

Pusat Teknologi Informasi dan Pangkalan Data

UIN Maulana Malik Ibrahim Malang

Jl. Gajayana No.50, Kota Malang ptipd.uin-malang.ac.id

Lembar Pengesahan

IDENTITAS DOKUMEN

- **Nama Dokumen:** SOP Penanganan Insiden Keamanan E-Journal (OJS)
- **Kode Dokumen:** 174-PTIPD-2026/07
- **Versi / Revisi:** 1.0
- **Tanggal Berlaku:** 27 Juli 2026

PERNYATAAN PENGESAHAN

Dengan ini menyatakan bahwa dokumen **SOP Penanganan Insiden Keamanan E-Journal (OJS)** ini telah diperiksa, disetujui, dan disahkan. Dokumen ini berlaku sebagai acuan teknis dan operasional resmi dalam penanganan insiden siber pada layanan e-journal di lingkungan **UIN Maulana Malik Ibrahim Malang** terhitung sejak tanggal ditetapkan.

Seluruh pengguna diharapkan mematuhi panduan ini guna menjamin keamanan informasi, standarisasi prosedur, serta optimalisasi pemanfaatan layanan teknologi informasi secara tertib dan akuntabel.

Ditetapkan di: Malang Pada Tanggal: 27 Juli 2026

Disusun Oleh,	**Disahkan Oleh,** Kepala PTIPD
Ainur Rahmawati	**Abid Yusron**
NIP. 198403132009012007	NIP. 19840409 201101 1 013

Daftar Isi

Pendahuluan

A. Deskripsi layanan

Open Journal Systems (OJS) merupakan platform manajemen e-journal berbasis web yang di-hosting pada infrastruktur server PTIPD UIN Maulana Malik Ibrahim Malang. Dokumen Standar Operasional Prosedur (SOP) ini disusun sebagai pedoman teknis pengelolaan respons insiden keamanan siber (*cyber incident response*) guna menjaga integritas data dan keberlangsungan layanan publik.

B. Tujuan dan manfaat

Penyusunan panduan dan penerapan SOP ini bertujuan untuk:

1. Menjamin aspek *Confidentiality, Integrity, and Availability* (CIA Triad) pada infrastruktur e-journal (Open Journal Systems/OJS) di lingkungan UIN Maulana Malik Ibrahim Malang.
2. Menetapkan pembagian peran (*Service Level Agreement* / SLA) yang jelas antara Journal Manager sebagai administrator aplikasi dan PTIPD sebagai pengelola infrastruktur server.
3. Menerapkan tindakan isolasi teknis berupa penangguhan sementara (*temporary suspension*) terhadap instance OJS yang terindikasi terinjeksi konten ilegal demi menjaga reputasi dan indeksibilitas institusi.

C. Ruang lingkup pengguna

SOP ini mencakup penanganan insiden keamanan siber, meliputi *web defacement*, link judol, penyebaran *malware*, *unauthorized user registration*, hingga kompromi kredensial akun pada platform OJS di bawah naungan UIN Maulana Malik Ibrahim Malang.

KEBIJAKAN PENGGUNA OJS

A. Pengelolaan Akun dan Autentikasi

1. **Manajemen Kredensial:** Journal Manager wajib menjaga kerahasiaan hak akses tingkat administrator (*Journal Manager/Site Admin*) dan menerapkan kebijakan kata sandi yang kuat (*strong password policy*).
2. **Eliminasi Akun Anomali:** Journal Manager secara berkala wajib melakukan *audit trail* dan mengeliminasi pendaftaran akun pengguna yang tidak sah (*unauthorized/spam users*).
3. **Restriksi Pendaftaran:** Apabila terdeteksi serangan *automated bot registration*, Journal Manager wajib mematikan fitur *user self-registration* pada konfigurasi OJS.

B. Pengawasan Konten dan Metadata

1. **Monitoring Integritas Konten:** Journal Manager bertanggung jawab penuh atas pengawasan konten harian pada jurnal masing-masing, termasuk naskah, metadata artikel, dan komentar.
2. **Pencegahan Injeksi Kode Malisios:** Dilarang keras mengunggah atau membiarkan eksekusi skrip malicious, *backdoor*, *phishing link*, maupun materi judol pada sistem OJS.
3. **Pembersihan Data (Data Sanitization):** Dalam kondisi terindikasi insiden, Journal Manager wajib melakukan pembersihan mandiri secara komprehensif pada tabel basis data (*database tables*) dan direktori penyimpanan berkas (*files directory*).

C. Kebijakan Akses Jaringan dan Mitigasi Siber

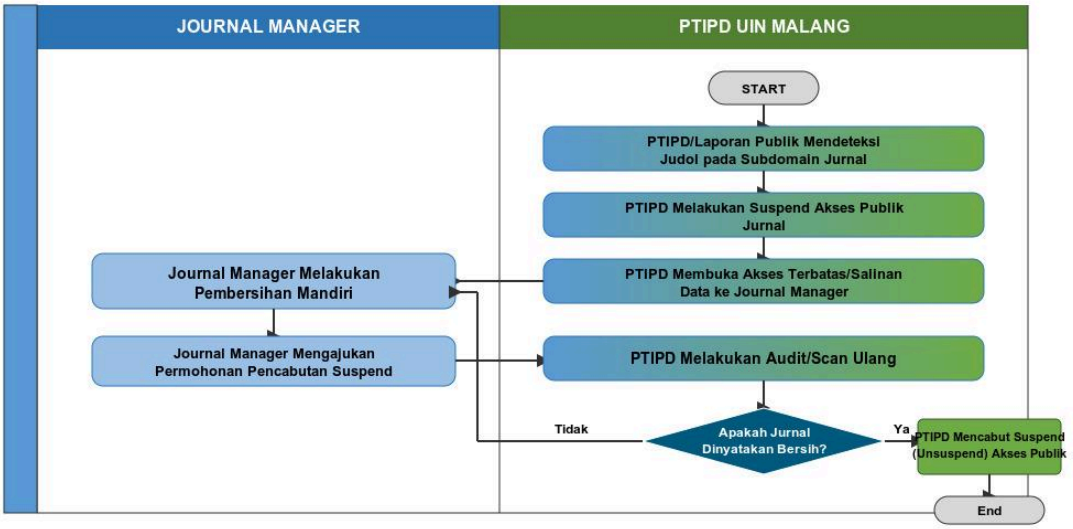
1. **Akses Operasional Normal:** Dalam kondisi aman, aplikasi bersifat *public-facing* dan dapat diakses secara luas melalui *Content Delivery Network* / ISP publik.
2. **Isolasi Siber Kritis:** Saat insiden terdeteksi, PTIPD berhak melakukan isolasi tingkat jaringan (*network isolation*) atau pemblokiran domain (*domain suspension*) secara seketika untuk mencegah *indexing* buruk oleh mesin pencari.
3. **Restriksi Akses IP:** Selama fase rekayasa pembersihan (*remediation phase*), akses ke dasbor OJS dibatasi terbatas pada daftar alamat IP terverifikasi (*IP whitelisting*) atau melalui enkripsi jaringan VPN institusi.

PROSEDUR OPERASIONAL PENANGANAN INSIDEN

A. Peran dan Tanggung Jawab

1. **Journal Manager (Application Layer):** Penanggung jawab eksekusi remediasi tingkat aplikasi, mencakup pembersihan *spam accounts*, *purging* metadata terinfeksi, manipulasi registrasi user, dan sanitasi konten.
2. **PTIPD UIN Malang (Infrastructure & Network Layer):** Penanggung jawab pengawasan lalu lintas jaringan (*traffic monitoring*), mitigasi ancaman server, isolasi sistem (*suspension*), serta verifikasi akhir kebersihan infrastruktur (*post-incident audit*).

B. Prosedur Khusus Penanganan Insiden Judi Online (Judol)



Gambar 1: Flowchart Alur Penanganan Insiden OJS

Deteksi & Tindakan Penangguhan (Suspend)

1. Apabila *Intrusion Detection System* (IDS) PTIPD atau laporan publik mendeteksi *gambling link injection* (tautan judol) atau aktivitas anomali pada subdomain jurnal, **PTIPD segera mengeksekusi penangguhan akses publik (suspend)**.
2. Langkah pemblokiran ini bertujuan meminimalisir dampak *SEO poisoning* serta implikasi hukum pada institusi.

Pembersihan Mandiri oleh Journal Manager

1. **Journal Manager melakukan proses sanitasi data secara menyeluruh** (*purging* akun spammer, pembersihan metadata artikel terinjeksi tautan malisios/judol, dan deaktivasi fitur registrasi publik).

Security Assessment & Pembukaan Normalisasi (Unsuspend)

1. Setelah proses pembersihan dinyatakan selesai oleh Journal Manager, permohonan resmi pencabutan status *suspend* diajukan kepada PTIPD.
2. PTIPD melakukan *vulnerability scanning* dan *security audit* ulang pada server serta basis data OJS. Jika hasil pemindaian mengonfirmasi sistem telah steril, PTIPD memulihkan akses publik (*unsuspend/re-enable*).

C. Matriks Tanggung Jawab Insiden

Kategori Insiden	**Kewajiban Journal Manager (App Level)**	**Kewajiban PTIPD (Server & Network Level)**
Terinjeksi Konten / Spam Judol	**Eksekutor Remediation:** Melakukan pembersihan akun ilegal, sanitasi metadata, dan eliminasi file terinfeksi hingga tuntas.	**Eksekutor Keamanan Infrastructure:** Mengisolasi sistem (*suspend*) dari jaringan publik, memberikan akses terbatas, serta melakukan *security re-assessment*.
Corrupted Core Files / Degradasi Hosting	Menganalisis dan melaporkan detail kegagalan fungsi aplikasi kepada Helpdesk PTIPD.	**Eksekutor Utama Infrastructure:** Melakukan perbaikan *core system*, alokasi *server resource*, dan eksekusi *disaster recovery / backup restoration*.

Kendala Umum & Layanan Bantuan

A. FAQ & *troubleshooting*

Berikut adalah beberapa kendala yang mungkin Anda temui beserta solusinya:

Tanya: Mengapa situs e-journal kami tiba-tiba di-*suspend* dan tidak dapat diakses publik?
Jawab: Hal ini menandakan sistem monitoring mendeteksi adanya indikasi siber/spam judi online pada subdomain jurnal Anda. Segera koordinasi dengan PTIPD untuk mendapatkan akses pembersihan mandiri.

Tanya: Apa yang harus dilakukan setelah Journal Manager selesai membersihkan file/user judol?
Jawab: Ajukan permohonan tertulis pencabutan *suspend* ke PTIPD agar dilakukan audit ulang dan pembukaan kembali (*unsuspend*) akses publik.

Tanya: Bagaimana jika terjadi kerusakan *file core* pada sistem OJS kami?
Jawab: Laporkan detail kerusakan kepada helpdesk PTIPD agar tim server dapat melakukan pemeliharaan atau pemulihan *backup* data.

B. Daftar layanan bantuan

Instruksi: Jangan mengubah informasi kontak di bawah ini, karena merupakan kanal resmi institusi. Anda dapat menambahkan jam operasional jika diperlukan.

Jika kendala yang Anda alami belum tercantum pada bagian FAQ atau memerlukan bantuan teknis lebih lanjut, Anda dapat menghubungi tim bantuan PTIPD melalui kanal resmi berikut:

1. Sistem Pengaduan Masyarakat (Dumas):
   Silakan sampaikan keluhan atau kendala Anda melalui portal:
   dumas.uin-malang.ac.id
2. WhatsApp Resmi UIN Malang:
   Layanan pesan singkat melalui nomor: +62816561337
3. Email Resmi PTIPD:
   Kirimkan detail kendala beserta tangkapan layar (screenshot) ke alamat: ptipd@uin-malang.ac.id atau kunjungi situs ptipd.uin-malang.ac.id