

LAPORAN PENANGANAN INSIDEN

Berdasarkan Form Rekap Insiden ISMS ISO/IEC 27001:2022
Diskominfo Kabupaten Klaten
Periode TW2 (April-Juni 2026)

1. Pendahuluan

Laporan ini disusun untuk memantau efektivitas penanganan insiden keamanan informasi berdasarkan form rekap insiden Diskominfo Kabupaten Klaten. Pemantauan dilakukan dengan acuan standar ISO/IEC 27001:2022 dan regulasi nasional yang berlaku. Tujuan laporan adalah memastikan bahwa insiden yang terjadi telah diidentifikasi dan dapat dikendalikan melalui implementasi keamanan informasi yang memadai.

2. Metodologi

Metodologi penanganan insiden dilakukan melalui langkah-langkah berikut:

1. Menggunakan form pelaporan insiden sebagai dasar pelaporan adanya insiden yang terjadi.
2. Penanganan insiden dilakukan oleh tim Manajemen Insiden
3. Merekap seluruh insiden pada form rekap insiden

3. Hasil Penanganan Insiden

No	Tanggal Pelaporan	Kategori Insiden	Deskripsi	Analisis Penyebab	Tindak Lanjut	Tanggal Selesai Perbaikan	Status
1	20/04/2026	Low Impact	Insecure Direct Object Reference (IDOR)	kontrol akses (otorisasi) yang tidak memadai pada sisi server	1. Terapkan pengecekan hak akses (RBAC) pada setiap request ke endpoint ini. 2. Gunakan UUID atau token acak sebagai parameter, bukan angka berurutan	20/04/2026	Tutup

4. Pembelajaran dari Insiden

- Pembelajaran penting (lessons learned) dari insiden IDOR adalah keamanan aplikasi tidak boleh berasumsi bahwa pengguna akan selalu bersikap jujur dan mengikuti alur yang sudah disediakan di antarmuka (UI).

5. Kesimpulan

Kerentanan Insecure Direct Object Reference (IDOR) terjadi akibat ketiadaan validasi otorisasi di sisi server ketika pengguna meminta akses ke objek internal sistem. Berikut adalah tiga poin esensial sebagai rangkuman: Akar Masalah: Aplikasi web terlalu mempercayai input pengguna (seperti parameter ID di URL) tanpa memeriksa apakah pengguna yang aktif benar-benar pemilik sah dari data tersebut. Dampak Utama: Menyebabkan kebocoran data massal, manipulasi informasi, hingga pengambilalihan akun secara ilegal. Solusi Mutlak: Terapkan pemeriksaan otorisasi yang ketat pada sisi server untuk setiap request, dan sembunyikan ID internal database menggunakan string acak seperti UUID.

Tanggal : 7 Juli 2026

Mengetahui :

Kepala Bidang Informatika dan Persandian

Kepala Dinas Komunikasi Dan Informatika
Kabupaten Klaten



Heri Wismo Handono. S.E, M.M
NIP 196901071989031003



Aris Pramana, S.E., M.M
NIP 197507182005011006