



SOP PENANGANAN INSIDEN SIBER

DINAS KEPEMUDAAN DAN OLAHRAGA PROVINSI JAWA TENGAH

A. Tujuan

SOP ini disusun sebagai pedoman bagi seluruh unsur di lingkungan Dinas Kepemudaan dan Olahraga Provinsi Jawa Tengah dalam melakukan penanganan insiden siber secara cepat, terkoordinasi, terdokumentasi dan bertanggung jawab.

SOP bertujuan untuk :

- mendeteksi insiden siber sedini mungkin
- mencegah meluasnya dampak insiden
- melindungi data dan sistem elektronik Dispora Jateng
- memulihkan sistem dan layanan yang terdampak
- memastikan tersedianya dokumentasi penanganan insiden
- melakukan pelaporan sesuai ketentuan yang berlaku
- menggunakan hasil evaluasi sebagai bahan peningkatan keamanan sistem.

Peraturan BSSN 1/2024 menempatkan penanganan insiden dalam kerangka penanggulangan, pemulihan, penyampaian informasi kepada pihak terkait, serta diseminasi informasi untuk mencegah atau mengurangi dampak insiden

B. Ruang Lingkup

SOP berlaku untuk sistem elektronik, aplikasi, jaringan, perangkat, akun dan data yang berada dalam pengelolaan atau digunakan untuk mendukung pelaksanaan tugas Dispora Provinsi Jawa Tengah.

Contohnya :

- website resmi Dispora Jateng
- aplikasi/Sistem Informasi Dispora
- SIMPORA
- server dan database
- jaringan internet dan jaringan internal
- komputer/laptop kedinasan
- akun email kedinasan
- akun media sosial resmi
- perangkat penyimpanan data
- sistem administrasi dan layanan digital
- data pegawai
- data atlet/peserta kegiatan
- dokumen kedinasan dalam bentuk elektronik
- sistem elektronik lain yang digunakan dalam pelaksanaan tugas dan pelayanan publik

C. Jenis Insiden Siber

Insiden yang dapat ditangani melalui SOP ini antara lain:

1. Peretasan : Akses tidak sah terhadap website, aplikasi, server, akun atau sistem Dispora.
2. Malware/Ransomware : Masuknya perangkat lunak berbahaya yang dapat merusak, mengenkripsi, menghapus atau mengganggu sistem dan data.
3. Kebocoran Data : Data atau dokumen yang seharusnya dilindungi diakses atau tersebar tanpa kewenangan.

4. Serangan Website/Aplikasi : Website atau aplikasi tidak dapat digunakan, mengalami perubahan tampilan tanpa kewenangan atau terdapat aktivitas mencurigakan.
5. Phishing/Social Engineering :Upaya memperoleh akun, kata sandi, kode OTP, atau informasi lainnya melalui pesan, email, tautan, atau manipulasi pengguna.
6. Serangan Jaringan : Gangguan atau aktivitas tidak sah terhadap jaringan komputer Dispora.
7. Insiden lainnya : Setiap kejadian keamanan informasi yang berpotensi mengganggu kerahasiaan, keutuhan, atau ketersediaan sistem dan data.

D. Tahapan Penanganan

1. DETEKSI

Tujuan: menemukan dan mengidentifikasi indikasi insiden siber.

Indikasi dapat diketahui melalui :

- laporan pegawai
- laporan masyarakat/pengguna layanan
- notifikasi keamanan system
- pemantauan website dan aplikasi
- pemantauan jaringan
- antivirus/security tools
- informasi dari BSSN atau pihak berwenang
- hasil pemeriksaan administrator system

Contoh kejadian :

Pegawai Dispora menemukan bahwa website resmi berubah tampilan secara tidak wajar.

Pegawai kemudian: Tidak melakukan perubahan sendiri → menyimpan informasi kejadian → segera melaporkan kepada pengelola/TIM terkait.

Output tahap deteksi

- laporan awal insiden
- waktu kejadian
- sistem yang terdampak
- indikasi awal
- identitas pelapor
- bukti awal seperti screenshot/log apabila tersedia.

2. RESPONS

Tujuan: mengendalikan insiden agar tidak semakin meluas.

Tindakan yang dapat dilakukan sesuai kondisi:

a. Amankan sistem terdampak

Misalnya memisahkan perangkat atau sistem yang terindikasi terkena serangan.

b. Blokir akses mencurigakan

Melakukan pemblokiran akun, alamat IP, akses, atau koneksi yang teridentifikasi mencurigakan sesuai kewenangan.

c. Isolasi perangkat

Jika diperlukan, perangkat yang diduga terinfeksi dipisahkan dari jaringan.

d. Lindungi bukti

Bukti digital, log, screenshot, waktu kejadian, dan informasi teknis tidak boleh sembarangan dihapus.

e. Koordinasi

Koordinasi dilakukan dengan :

- ✓ pengelola TI
- ✓ administrator system
- ✓ pejabat/unit terkait
- ✓ Tim Tanggap Insiden Siber apabila telah dibentuk/ditetapkan
- ✓ pengelola SPBE/keamanan informasi Pemerintah Provinsi Jawa Tengah
- ✓ pihak berwenang/BSSN sesuai ketentuan.

Prinsip penting

Cepat – Terukur – Tidak Panik – Tidak Menghilangkan

3. PEMULIHAN

Tujuan: mengembalikan sistem dan layanan Dispora ke kondisi aman dan normal.

Tahap pemulihan meliputi:

- a. Pemeriksaan sumber masalah : Identifikasi penyebab dan titik masuk insiden.
- b. Pembersihan : Menghapus malware, akun ilegal, konfigurasi berbahaya, atau komponen lain yang menyebabkan insiden setelah bukti yang diperlukan diamankan.
- c. Pemulihan dari backup : Jika sistem atau data rusak, dilakukan pemulihan menggunakan backup yang tersedia dan tervalidasi.
- d. Pengujian : Sebelum layanan dibuka kembali, dilakukan pengujian:
 - fungsi aplikasi
 - keamanan
 - integritas data
 - akun dan hak akses
 - jaringan dan layanan yang terkait.
- e. Pengaktifan kembali layanan : Layanan dikembalikan secara bertahap setelah dinyatakan aman oleh pihak yang berwenang.

Peraturan BSSN 1/2024 mengatur agar organisasi memiliki rencana tanggap insiden dan keberlangsungan kegiatan, termasuk strategi, tahapan, target waktu pemulihan, sumber daya, personel, serta pelaksanaan simulasi secara berkala.

4. PELAPORAN

Setelah insiden diidentifikasi dan ditangani sesuai tingkat risikonya, dilakukan dokumentasi dan pelaporan.

Laporan internal minimal memuat:

- a. identitas pelapor
- b. tanggal dan waktu kejadian
- c. jenis insiden
- d. sistem/perangkat yang terdampak
- e. kronologi
- f. indikasi penyebab
- g. dampak
- h. tindakan yang telah dilakukan
- i. kondisi terakhir
- j. kebutuhan tindak lanjut dan bukti pendukung.

Peraturan BSSN 1/2024 menetapkan bahwa laporan insiden sekurang-kurangnya memuat informasi kontak pelapor, deskripsi insiden, kronologi dan dampak serangan untuk insiden yang memenuhi kriteria pelaporan.

Pelaporan eksternal

Untuk insiden yang memenuhi kriteria pelaporan sesuai ketentuan, dilakukan penyampaian laporan kepada pihak yang berwenang melalui mekanisme/kanal yang ditetapkan.

Peraturan BSSN 1/2024 mengatur bahwa insiden yang memenuhi ketentuan pelaporan disampaikan oleh Tim Tanggap Insiden Siber organisasi kepada Tim Tanggap Insiden Siber sektoral dengan tembusan kepada Tim Tanggap Insiden Siber nasional.

5. EVALUASI

Tahap ini penting dan sebaiknya tetap dipertahankan seperti pada poster yang dibuat.

Setelah insiden selesai, evaluasi meliputi :

Apa yang terjadi?

- Jenis insiden
- sistem yang terkena
- waktu kejadian.

Mengapa terjadi?

- celah keamanan
- kesalahan konfigurasi
- kelemahan system
- kelalaian pengguna
- serangan eksternal atau faktor lain yang teridentifikasi.

Bagaimana penanganannya?

- tindakan yang dilakukan
- waktu respons
- efektivitas Tindakan
- kendala yang ditemukan.

Apa yang perlu diperbaiki?

- keamanan system
- backup
- pengaturan akses
- SOP
- kompetensi SDM
- monitoring
- perangkat keamanan.

Hasil evaluasi kemudian digunakan sebagai bahan perbaikan berkelanjutan dan pencegahan kejadian serupa.



SOP PENANGANAN INSIDEN SIBER

Deteksi – Respons – Pemulihan – Pelaporan

(Mengacu pada Peraturan BSSN No. 8 Tahun 2020 dan No. 1 Tahun 2024)

SOP ini menjadi panduan bagi seluruh pihak di lingkungan Dispora Provinsi Jawa Tengah untuk menangani insiden siber secara cepat, tepat, dan terkoordinasi.

