

PANDUAN PELAPORAN INSIDEN SIBER

DIREKTORAT PENANGGULANGAN
DAN PEMULIHAN PEMERINTAH





VERSI DOKUMEN

| No | Tanggal | Versi Dokumen | Oleh | Keterangan |
|----|---------------|---------------|----------------|------------|
| 1 | Desember 2018 | Versi 0 | Direktorat PPP | - |
| | | | | |
| | | | | |
| | | | | |



KATA PENGANTAR

Puji syukur kehadiran Allah SWT, atas segala limpahan rahmat, nikmat serta karunia-Nya yang tak ternilai dan tak dapat dihitung sehingga kami dapat menyelesaikan penyusunan “Panduan Pelaporan Insiden Siber”. Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam pelaporan insiden siber. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi insiden siber, yang dimulai dari tahap pelaporan sampai dengan tahap penutupan tiket. Panduan ini tentu saja masih banyak kekurangan dan masih jauh dari kesempurnaan karena keterbatasan ilmu dan referensi kami. Untuk itu, kami selalu berusaha melakukan evaluasi dan perbaikan secara berkala agar bisa mencapai hasil yang lebih baik lagi.

Akhir kata, kami ucapkan terima kasih kepada segala pihak yang telah membantu dalam penyusunan panduan ini.

Jakarta, Desember 2018
Deputi III,

Asep Chaerudin, M.A.S.S



DAFTAR ISI

| | |
|---|----------|
| 1. TUJUAN | 1 |
| 2. RUANG LINGKUP | 1 |
| 3. PROSEDUR PELAPORAN INSIDEN..... | 2 |
| 3.1 Laporan Insiden Siber..... | 2 |
| 3.2 Verifikasi Insiden Siber | 3 |
| 3.3 Approvement | 3 |
| 3.4 Open Ticket | 3 |
| 3.5 Respon Insiden | 4 |
| 3.6 Close Ticket | 4 |



PANDUAN PELAPORAN INSIDEN

1. TUJUAN

Penanganan yang terencana dan terorganisir sangatlah diperlukan dalam hal terjadinya sebuah insiden, supaya hal tersebut dapat dilakukan, maka diperlukan adanya suatu prosedur yang standar dalam melakukan pelaporan insiden tersebut. Secara umum, tujuan prosedur pelaporan insiden ini adalah sebagai panduan untuk pengelola Teknologi Informasi jika terjadi insiden dan sebagai dokumentasi untuk setiap insiden yang terjadi dalam proses pengelolaan Teknologi Informasi.

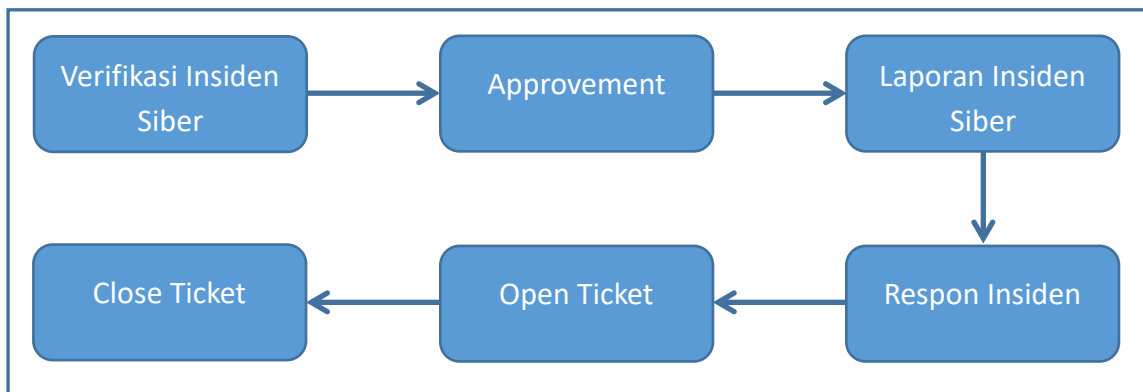
2. RUANG LINGKUP

Prosedur Pelaporan Insiden ini berisi tentang langkah-langkah yang dilakukan pada saat terjadi insiden dan melaporkan insiden tersebut kepada Badan Siber dan Sandi Negara (BSSN). Dalam pelaporan insiden, pusat kontak insiden siber dari BSSN adalah Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas).

Pusopskamsinas akan melanjutkan ke Deputi Bidang Penanggulangan dan Pemulihan untuk menangani insiden yang dilaporkan. Laporan insiden yang ditangani dapat berasal dari Sektor Pemerintah, Sektor Infrastruktur Informasi Kritis Nasional, dan Ekonomi Digital.

3. PROSEDUR PELAPORAN INSIDEN

Secara umum tahapan dalam melakukan pelaporan insiden siber dapat digambarkan sebagai berikut :



Gambar 1. Tahap Pelaporan Insiden

3. 1. Laporan Insiden Siber

Pelapor yang dalam hal ini pengelola IT yang terkena insiden ataupun pengguna yang menemukan adanya insiden, dapat dilakukan melalui alamat email pusopskamsinas@bssn.go.id atau bantuan70@bssn.go.id atau dapat menghubungi via telepon di (021)78833610. Pelapor dapat melampirkan bukti insiden, berupa screenshot insiden.

3. 2. Verifikasi Insiden Siber

Berdasarkan laporan insiden siber tersebut, Pusopskamsinas akan melakukan verifikasi insiden tersebut. Tahap verifikasi dilakukan dengan cara pihak pengelola website tersebut mengisi data-data lengkap seperti identitas lengkap pengelola website, jenis insiden, sistem log aplikasi, dan dampak terkait insiden tersebut.

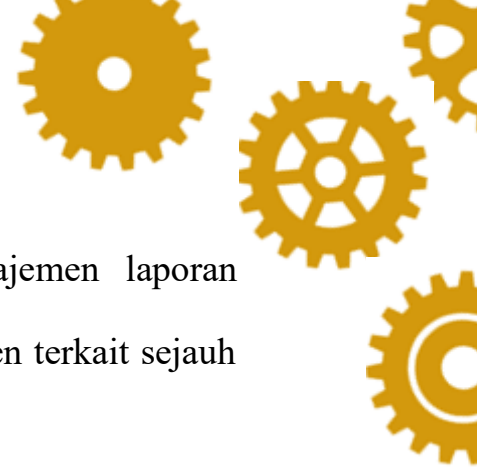
Tujuan dari tahap Verifikasi ini adalah melakukan identifikasi dari insiden yang terjadi dan melakukan dokumentasi terhadap insiden tersebut.

3. 3. Approvement

Laporan insiden siber yang telah diverifikasi akan dilakukan approvement guna untuk penanganan insiden selanjutnya. Approvement dilakukan oleh pimpinan pada Pusopskamsinas.

3. 4. Open Ticket

Setelah dilakukan verifikasi dan dinyatakan valid, maka akan diberlakukan sistem *open ticket*. Tiket tersebut berisi informasi mengenai nomor tiket insiden dan informasi terkait penanganan insiden. Tiket yang telah dibuat, nantinya akan dilanjutkan ke tim *Response Incident BSSN*.



Tiket ini bertujuan untuk melakukan manajemen laporan insiden dan dapat sebagai monitoring pelapor insiden terkait sejauh mana insiden tersebut ditangani oleh BSSN.

3. 5. Respon Insiden

Tim respon insiden akan melakukan koordinasi dengan pihak pengelola IT terkait dengan tiket tersebut. Tim respon insiden akan memberikan panduan terkait mekanisme penanggulangan dan pemulihan website tersebut. Jika diperlukan penanganan khusus, maka tim dapat melakukan penanggulangan dan pemulihan website tersebut secara on-site. Pada tahapan ini, akan dihasilkan berupa rekomendasi penanggulangan dan pemulihan terkait insiden yang terjadi.

3. 6. Close Ticket

Selanjutnya, pihak pengelola website dapat melakukan penanggulangan dan pemulihan sesuai dengan rekomendasi yang telah diberikan. Tim akan melakukan pantauan terhadap website yang terkena insiden tersebut. Jika insiden telah dapat diatasi, maka akan dilakukan Close Ticket.