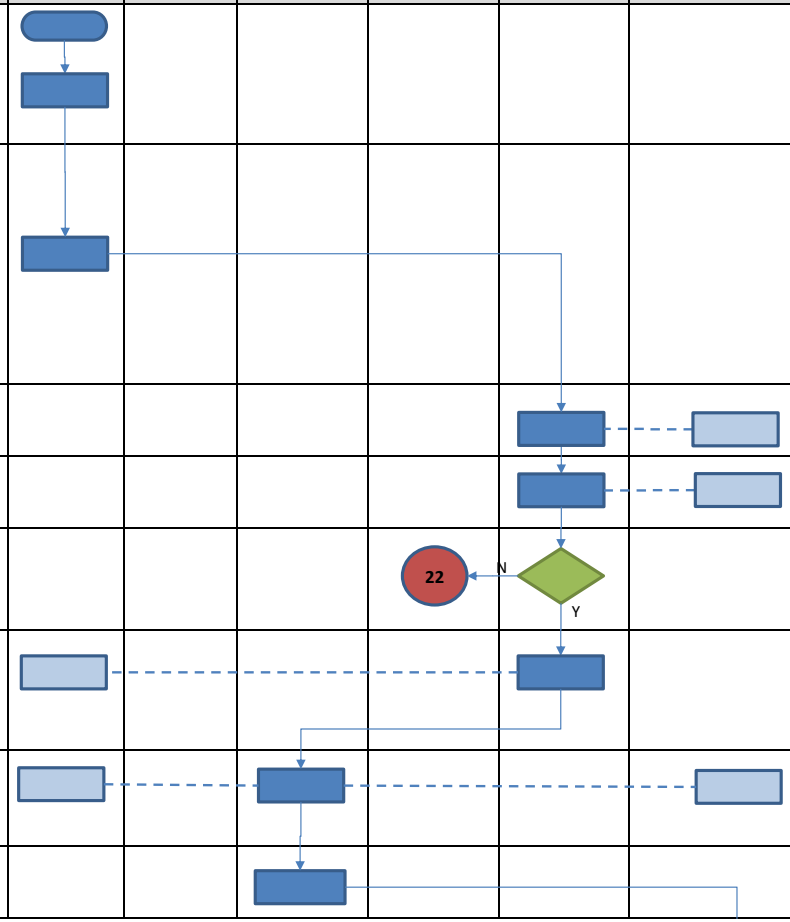
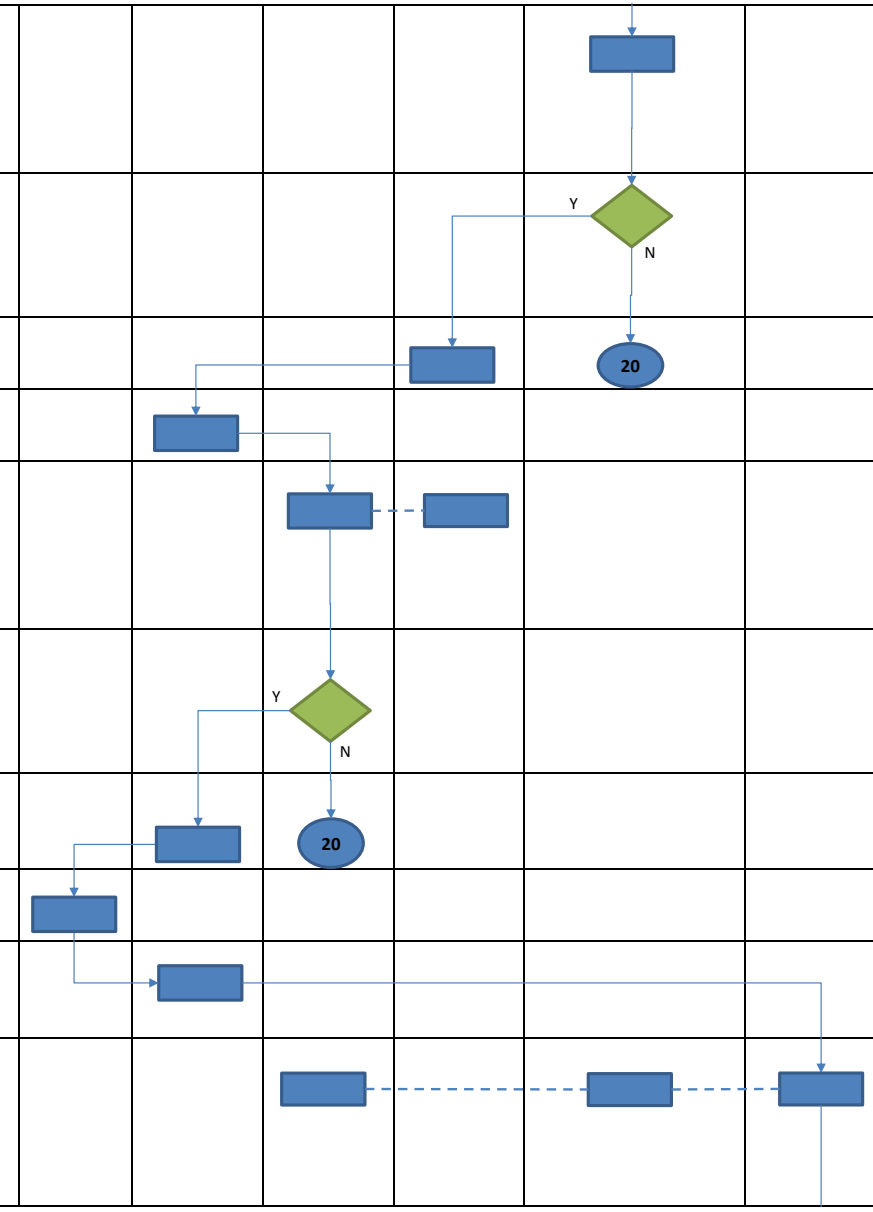
LAMPIRAN
Nota Dinas Kepala Pusat Data dan Teknologi Informasi
Nomo : SEK.7-TI.03.01-02
Tanggal: 15 Maret 2022

# STANDAR OPERASIONAL PROSEDUR
# PENANGANAN INSIDEN SIBER DI LINGKUNGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

| No | Kegiatan | PELAKSANA | | | | | | | MUTU BAKU | | | KETERANGAN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Pemohon | Ketua KUMHAM-CSIRT (Kapusdatin) | Koordinator KUMHAM-CSIRT (koor. Bidjar) | Anggota KUMHAM-CSIRT Pusdatin | PIC Unit Utama (TEAM LEADER) | Anggota KUMHAM-CSIRT Unit Utama | Pihak Eksternal (CSIRT Nasional) | Input | Waktu | Output | |
| 1 | Terjadi insiden siber | | | | | | | | | | | |
| 2 | Membuat ticket pelaporan insiden | | | | | | | | 1. informasi pelaporan insiden; 2. bukti insiden; | 30 menit | Ticket Pelaporan | melalui website ticket pelaporan insiden.<br><br>Bukti insiden:<br>- screenshoot<br>- log aplikasi<br>- Reimaging OS<br>- Database<br>- dll |
| 3 | Menindaklanjuti tiket pelaporan | | | | | | | | Ticket Pelaporan | 30 menit | Ticket Pelaporan dan Informasi Laporan Insiden | melalui website ticket. |
| 4 | Memeriksa gangguan pada laporan ticket | | | | | | | | Ticket Pelaporan dan Informasi Laporan Insiden | 2 jam | Jurnal insiden keamanan | |
| 5 | Mengevaluasi kebenaran gangguan insiden siber | | | | 22 | N / Y | | | Jurnal insiden keamanan | 1 jam | Hasil evaluas | lewat aplikasi dengan perubahan status |
| 6 | Mengirimkan pemberitahuan kepada Pemilik / Penanggung-Jawab Aset tentang adanya insiden siber kepada unit kerja dan koordinator CSIRT | | | | | | | | Hasil evaluasi | 30 menit | Hasil pemberitahuan | lewat aplikasi dengan perubahan status |
| 7 | Menganalisis insiden keamanan yang dilaporkan dengan menentukan prioritas dan rencana penanganan | | | | | | | | Hasil pemberitahuan | 1 jam | Log gangguan insiden siber | |
| 8 | Menunjuk anggota KUMHAM-CSIRT untuk melakukan penanganan | | | | | | | | Log gangguan insiden siber | 30 menit | Disposisi | |



| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **9** | Penanganan secara teknis | | | | | | | | Disposisi | 1 hari | Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dan tindak lanjut di Unit Utama | Meliputi tindakan<br>- Penahanan (containment);<br>- Penghapusan konten (eradication);<br>- Pemulihan |
| **10** | Terjadi kendala dalam penanganan secara teknis | | | | | | | | Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dan tindak lanjut di | 1 jam | Laporan kendala penanganan di Unit Utama | |
| **11** | Melaporkan kendala dalam penanganan insiden siber | | | | | | | | Laporan kendala penanganan di Unit Utama | 30 menit | Laporan dan Log penanganan insiden siber | lewat aplikasi dengan perubahan status |
| **12** | Mengevaluasi kebutuhan penanganan insiden siber | | | | | | | | Laporan dan Log penanganan insiden siber | 1 jam | Disposisi dan Arahan | |
| **13** | Penanganan secara teknis oleh pusdatin | | | | | | | | Disposisi dan Arahan | 1 hari | Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dan tindak lanjut di Pusdatin | Meliputi tindakan<br>- Penahanan (containment);<br>- Penghapusan konten (eradication);<br>- Pemulihan |
| **14** | Terjadi kendala dalam penanganan secara teknis | | | | | | | | Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dan tindak lanjut di | 1 jam | Laporan kendala penanganan di unit utama dan pusdatin | |
| **15** | Melaksanakan langkah-langkah yang diperlukan untuk mendapat bantuan eksternal. | | | | | | | | Laporan kendala penanganan di unit utama dan pusdatin | 1 jam | Surat dan Dokumen laporan penanganan insiden siber | |
| **16** | Menghubungi pihak eksternal untuk mendapatkan bantuan penanganan | | | | | | | | Surat dan Dokumen laporan penanganan insiden siber | 30 menit | Respon pihak luar | |
| **17** | Menunjuk anggota KUMHAM-CSIRT untuk melakukan penanganan dengan bantuan pihak luar | | | | | | | | Respon pihak luar | 1 jam | Disposisi | |
| **18** | Penanganan secara teknis oleh Pihak Eksternal | | | | | | | | Disposisi | 2 hari | Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dan tindak lanjut di tingkat Eksternal | Meliputi tindakan<br>- Penahanan (containment);<br>- Penghapusan konten (eradication);<br>- Pemulihan |



| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **19** | Melakukan pencatatan detail penanganan dan pengumpuan dokumentasi | | | | | | | | Log penanganan insiden siber berupa laporan hasil penanganan, recovery, metode, dan tindak lanjut di tingkat Eksternal | 2 jam | Dokumentasi penanganan teknis | |
| **20** | Memeriksa kesesuaian penyelesaian insiden keamanan dan semua rincian insiden, tindakan-tindakan yang dilakukan, serta bukti-bukti insiden telah dicatat dan disimpan sesuai dengan ketentuan yang berlaku | | | | | | | | Dokumentasi penanganan teknis | 1 jam | Laporan teknis penyelesaian penanganan insiden | |
| **21** | Melaporkan penyelesaian teknis penanganan insiden | | | | | | | | Laporan teknis penyelesaian penanganan insiden | 10 menit | Laporan akhir penanganan insiden | |
| **22** | **Penutupan ticket pelaporan insiden siber** | | | | | | | | Laporan akhir penanganan insiden | 5 menit | 1. dokumen penutupan tiket<br>2. laporan akhir penanganan insiden | |

#KUMHAMPASTI

Ditandatangani secara elektronik oleh :
Hermansyah Siregar
NIP 197010161992031001

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara
Keaslian dokumen dapat dicek melalui tautan https://bsre.bssn.go.id/verifikasi