



Formulir Aduan Insiden Siber

A. INFORMASI UMUM	
1. Identitas Pelapor	
Nama Lengkap*	
Email*	
Telepon Organisasi*	
Handphone*	
Organisasi*	
2. Tipe Laporan (Pilih Salah Satu)	
<input type="checkbox"/> Awal <input type="checkbox"/> Lanjutan <input type="checkbox"/> Akhir	
3. Waktu Terjadinya Insiden	
Hari, Tanggal	
Pukul	
4. Tipe Insiden	
<input type="checkbox"/> Website Defacement <input type="checkbox"/> Un-patched Vulnerable Software Exploitation <input type="checkbox"/> Account Compromise <input type="checkbox"/> Unauthorized System Access <input type="checkbox"/> Patched Software Exploitation <input type="checkbox"/> Data Theft <input type="checkbox"/> Service Disruption <input type="checkbox"/> Malware Infection <input type="checkbox"/> Exploitation of Weak Configuration <input type="checkbox"/> Wireless Access Point Exploitation <input type="checkbox"/> Social Engineering and Phising Attacks. <input type="checkbox"/> Exploitation of Weak Network Architecture <input type="checkbox"/> Unintentional Information Exposure. <input type="checkbox"/> Network Penetration <input type="checkbox"/> Spoofing or DNS Poisoning <input type="checkbox"/> Lainnya	
5. Deskripsi Insiden disertai bukti (Screenshot, Domain Name, URL, Email, dll)	
6. Dampak Insiden	
<input type="checkbox"/> Jaringan Publik <input type="checkbox"/> Jaringan Internal <input type="checkbox"/> Lainnya	
7. Tindakan Penanggulangan Insiden	
a) Respon Cepat/Awal (Jangka Pendek)	
b) Jangka Panjang	
c)Apakah perencanaan BackUp System berhasil diimplementasikan? Jika iya, deskripsikan proses tersebut	

8. Apakah Organisasi lain dilaporkan? Jika iya, sebutkan			
B. INFORMASI KHUSUS			
9. Aset Kritis yang terkena dampak			
10. Dampak insiden terhadap aset			
<input type="checkbox"/> Data Theft System (Software/ Hardware) Sabotage		<input type="checkbox"/> Service Disruption (Downtime) <input type="checkbox"/> <input type="checkbox"/> Lainnya (Sebutkan)	
11. Jumlah Pengguna yang terkena dampak			
12. Dampak terhadap ICT (Information and Communication Technologies)			
13. Profil Penyerang			
a) IP address penyerang			
b) Port yang diserang			
14. Tipe Serangan			
<input type="checkbox"/> Website Defacement <input type="checkbox"/> Account Compromise <input type="checkbox"/> Patched Software Exploitation		<input type="checkbox"/> Unpatched Vulnerable Software Exploitation <input type="checkbox"/> Unauthorised System Access <input type="checkbox"/> Data Theft	
15. Analisis			
a) Laporan analisis log	<input type="checkbox"/> Ada	<input type="checkbox"/> Tidak Ada	<input type="checkbox"/> Sedang Proses
b) Laporan forensic	<input type="checkbox"/> Ada	<input type="checkbox"/> Tidak Ada	<input type="checkbox"/> Sedang Proses
c) Laporan audit	<input type="checkbox"/> Ada	<input type="checkbox"/> Tidak Ada	<input type="checkbox"/> Sedang Proses
d) Laporan analisis lalu lintas jaringan (Network Traffic)	<input type="checkbox"/> Ada	<input type="checkbox"/> Tidak Ada	<input type="checkbox"/> Sedang Proses
Rincian			
a) Nama dan versi Perangkat			
b) Lokasi Perangkat			
c) Sistem Operasi			
d) Terakhir update sistem operasi/firmware			

e) IP Address	
f) MAC Address	
g) DNS Entry	
h) Domain/Workgroup	
i) Apakah perangkat yang terkena dampak terhubung ke jaringan?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak
j) Apakah perangkat yang terkena dampak terhubung ke modem?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak
k) Adakah pengamanan fisik terhadap perangkat?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak
l) Adakah pengamanan logik terhadap perangkat?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak
m) Apakah perangkat sudah diputus dari jaringan?	<input type="checkbox"/> Ya <input type="checkbox"/> Tidak
16. Status Insiden	
17. Status Insiden	
18. Apakah sudah pernah ditawarkan sistem manajemen krisis?	

Catatan :

Segala informasi yang anda berikan tidak akan kami sebarluaskan kepada siapapun dan dijamin kerahasiaannya.

[*] : wajib diisi.