PEMERINTAH KABUPATEN HALMAHERA SELATAN
DINAS KOMINFO, STATISTIK DAN PERSANDIAN
Jl. Metro Sayoang KM Nol email : diskominfo@halmaheraselatankab.go.id
L A B U H A

Formulir Aduan Insiden Siber

A. INFORMASI UMUM	
1. Identitas Pelapor	
Nama Lengkap*	
Email*/url	
Telepon Organisasi*	
Handphone*	
Organisasi*	
2. Tipe Laporan (Pilih Salah Satu)	
☐ Awal ☐ Lanjutan ☐ Akhir	
3. Waktu Terjadinya Insiden	
Hari, Tanggal	
Pukul	
4. Tipe Insiden	
☐ Website Defacement / Pengrusakan Situs ☐ Account Compromise / Kompromi Akun ☐ Patched Software Exploitation/ Eksploitasi Software Yang Di tambal ☐ Service Disruption / Gangguan Pelayanan ☐ Exploitation of Weak Configuration/ Ekploitasi Configurasi Yang Lemah ☐ Social Engineering and Phising Attacks/ Rekayasa Sosial Dan Serangan Phising ☐ Unintentional Information Exposure/ Paparan Info yang Tidak Sengaja ☐ Spoofing or DNS Poisioning /Keracunan DNS	☐ Un-patched Vulnerable Software Exploitation/ Akses Software Yang Rentan ☐ Unauthorized System Access / Akses System Tidak Tepat ☐ Data Theft /Pencurian Data ☐ Malware Infection / Infeksi Perangkat Lunak Jahat ☐ Wireless Access Point Exploitation/ Eksploitasi Titik Akses Nirkabel ☐ Exploitation of Weak Network Architecture/ Eksploitasi Arsitektur Jaringan yang Lemah ☐ Network Penetration (Penterasi Jaringan) ☐ Lainnya
5. Deskripsi Insiden disertasi bukti (Screenshot, Domain Name, URL, Email, dll)	
6. Dampak Insiden	
☐ Jaringan Publik ☐ Jaringan Internal ☐ Lainnya	
7. Tindakan Penanggulangan Insiden	
a) Respon Cepat/Awal (JangkaPendek)	
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	
☐ Data Theft System (Software/ Hardware) Sabotage	☐ Service Disruption (Downtime) ☐ 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	
☐ Website Defacement/ Pengrusakan Situs ☐ Account Compromise/ Compromi Akun ☐ Patched Software Exploitation/ Eksplotasi Software Yang Ditambal	☐ Unpatched Vulnerable Software Exploitation/ Akses Sofware Yang Rentan ☐ Unauthorised System Access/ Akses System Yang Tidak Tepat ☐ Data Theft/ Pencurian Data
15. Analisis	
a) Laporan analisis log	☐ ☐ Tidak Ada ☐ Sedang Proses
b) Laporan forensic	☐ ☐ Tidak Ada ☐ Sedang Proses
c) Laporan audit	☐ ☐ Tidak Ada ☐ Sedang Proses

d) Laporan analisis lalu lintasjaringan (Network Traffic)	☐ ☐ Tidak Ada ☐ 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?	☐ Ya ☐ Tidak
j) Apakah perangkat yang terkena dampak terhubung ke modem?	☐ Ya ☐ Tidak
k) Adakah pengamanan fisik terhadap perangkat?	☐ Ya ☐ Tidak
l) Adakah pengamanan logik terhadap perangkat?	☐ Ya ☐ Tidak
m) Apakah perangkat sudah diputus dari jaringan?	☐ Ya ☐ 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.