# Formulir Aduan Insiden Siber
# SulbarProv-CSIRT

| A. INFORMASI UMUM | |
|---|---|
| **1. Identitas Pelapor** | |
| Nama Lengkap* | |
| Email* | |
| No. Telp Instansi* | |
| HP* | |
| Instansi* | |
| **2. Tipe Laporan (Pilih Salah Satu)** | |
| ☐ Awal ☐ Lanjutan ☐ Akhir | |
| **3. Waktu Terjadinya Insiden** | |
| Hari, Tanggal | |
| Pukul | |
| **4. Tipe Insiden** | |
| ☐ Website Defacement<br>☐ Account Compromise<br>☐ Patched Software Exploitation<br>☐ Service Disruption<br>☐ Exploitation of Weak Configuration<br>☐ Social Engineering and Phising Attacks.<br>☐ Unintentional Information Exposure.<br>☐ Spoofing or DNS Poisioning | ☐ Un-patched Vulnerable Software Exploitation<br>☐ Unauthorized System Access<br>☐ Data Theft<br>☐ Malware Infection<br>☐ Wireless Access Point Exploitation<br>☐ Exploitation of Weak Network Architecture<br>☐ Network Penetration<br>☐ 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 (Jangka Pendek) | |
| b) Jangka Panjang | |
| c) Apakah perencanaan | |

| | |
|---|---|
| BackUp System berhasil diimplementasikan?<br>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 □ Service Disruption (Downtime)<br>□ System (Software/ Hardware) Sabotage □ 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 □ Unpatched Vulnerable Software Exploitation<br>□ Account Compromise □ Unauthorised System Access<br>□ Patched Software Exploitation □ Data Theft |
| 15. Analisis |

| | | | |
|---|---|---|---|
| a) Laporan analisis log | □ Ada | □ Tidak Ada | □ Sedang Proses |
| b) Laporan forensic | □ Ada | □ Tidak Ada | □ Sedang Proses |
| c) Laporan audit | □ Ada | □ Tidak Ada | □ Sedang Proses |
| d) Laporan analisis lalu lintas jaringan (Network Traffic) | □ Ada | □ 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.*