	INCIDENT REPORT FORM **SUMBARPROV-CSIRT**	No. :

INCIDENT REPORT FORM	
Kategori Insiden (category of incident) :	Jenis insiden : [1] Web Defacement [2] Malware Attack [3] Phising [4] Spam [5] Denial of service [6] Probe scan [7] Lainnya, sebutkan: .....
	Catatan : pilih salah satu kategori insiden di atas
Pelapor (incident report by) :	Tanggal Laporan : …… Nama : …… Jabatan : …… NIP : …… No HP : …… Email : ……
Nama Instansi (institution by) :	Nama Instansi : Alamat Instansi : Telp./Fax : Email :
Mulai Tanggal dan Waktu Kejadian (starting date and time of incident) : Catatan : Tuliskan sesuai waktu setempat	Tanggal ……. Pk .....WIB
Lokasi insiden (location of incident) :	
Sistem yang terkena pengaruh insiden (systems effected due to the incident) :	Nama Sistem : Jenis Sistem : Server / Website / PC / Network URL : IP Address : OS : Web Server :
Deskripsi kejadian insiden (Description of the security incident) , disertai bukti / screenshot serangan	
Internet Services Provider (ISP) :	
Down time or system down jika ada (system down or down time, if any) :	[ya] [tidak] durasi waktu : catatan : jika ya, tuliskan durasi waktu, selain itu abaikan
Tindakan/teknis kebijakan yang sudah dilakukan atau Aduan Lanjutan :	(1)……, Tanggal …… (2)……, Tanggal …… (3))……., Tanggal …… Dst…
Rekomendasi Penanggulangan dan Pemulihan:	(1)……, Tanggal …… (2)……, Tanggal …… (3))……., Tanggal …… Dst…
Progress Penanganan Insiden	[1] Laporan Pertama [2] Sudah Direspon (On Progress), Tanggal …… [3] Eskalasi BSSN, Tanggal …… [4] Ditutup / Selesai, Tanggal ……

Keterangan Pengisi :
(*1) Owner Aplikasi
(*2) Helpdesk Dinas Komunikasi dan Informatika Provinsi Sumatera Barat
(*3) Tim Pengelolaan Data dan Koordinasi SumbarProv-CSIRT
(*4) Tim Penanggulangan dan Pembulihan Insiden SumbarProv-CSIRT
(*5) Tim Gulih SumbarProv-CSIRT Sub Pengelolaan Jaringan dan Server
(*6) Tim Gulih SumbarProv-CSIRT Sub Keamanan Informasi
(*7) Tim Gulih SumbarProv-CSIRT Sub Website Administrator dan Aplikasi

CONTOH PENGISIAN INCIDENT REPORT FORM

<table>
<tr><th colspan="2"><u>INCIDENT REPORT FORM</u></th></tr>
<tr><td rowspan="2">Kategori Insiden (category of incident) :
(*1)</td><td>Jenis insiden :
[1] web defacement (√)
[2] hacking
[3] malware attack
[4] phising
[5] spoofing
[6] brute force
[7] denial of service
[8] sniffing
[9] lainnya : …….</td></tr>
<tr><td>Catatan : pilih salah satu kategori insiden di atas</td></tr>
<tr><td>Pelapor (incident report by) :
(*1)</td><td>Tanggal Laporan : ……
Nama : ……
Jabatan : ……
NIP : ……
No HP : ……
Email : ……</td></tr>
<tr><td>Nama Instansi (institution by) :
(*1)</td><td>Nama Instansi : ……
Alamat Instansi : ……
Telp./Fax : ……
Email : ……</td></tr>
<tr><td>Mulai Tanggal dan Waktu Kejadian (starting date and time of incident) :

Catatan : Tuliskan sesuai waktu setempat</td><td>Tanggal 04-10-2019 (*1)</td></tr>
<tr><td>Lokasi insiden (location of incident) : (*1)</td><td>Server Hosting :
……</td></tr>
<tr><td>Sistem yang terkena pengaruh insiden (systems effected due to
the incident) : (*1)</td><td>Nama Sistem : ……
Jenis Sistem : Server / Website / PC / Network
URL : ……
IP Address : ……
OS : CentOS
Web Server : Apache 2.4.6</td></tr>
<tr><td>Deskripsi kejadian insiden (Description of the security incident) , disertai bukti / screenshot serangan :</td><td>1. Admin Web menemukan serangan defacement pada link …… (Gambar 1) (*1)
 
Gambar 1. Serangan Defacement pada</td></tr>
</table>

	Website ……
Internet Services Provider (ISP) : (*1)	……..
Down time or system down jika ada (system down or down time, if any) : (*1)	[ya] **[tidak]** durasi waktu : catatan : jika ya, tuliskan durasi waktu, selain itu abaikan
Tindakan teknis / kebijakan yang sudah dilakukan atau Aduan Lanjutan :	[1] Admin Web menemukan *site* dengan url.....yang terkena serangan *defacement.* (*1) **Tanggal** 04-10-2019 [2] Admin Web menghubungi Dinas Kominfo untuk memasukkan laporan insiden; (*1) **Tanggal** 24-10-2019 [3][3] **Tanggal** ……..
Rekomendasi Penanggulangan dan Pemulihan: (*4)	[1]
Progress Penanganan Insiden :	[1] **Temuan Server/Website/PC/Network yang Terkena pengaruh serangan** : *Jumat, 04-10-2019* (*1) [2] **Kontak Diskominfo** : *Kamis, 24-10-2019* (*1) [3] Laporan Pertama : *Kamis, 24-10-2019* (*1) [4] Sudah Direspon : [5] On Progress [6] Eskalasi BSSN : [7] Koordinasi ke ……, Tanggal ……. Dst….. [..] Ditutup / Selesai, Tanggal ……

Keterangan Pengisi:
(*1) Owner Aplikasi
(*2) Helpdesk Dinas Kominfo
(*3) Tim Pengelolaan Data dan Koordinasi JabarProv-CSIRT
(*4) Tim Analisis JabarProv-CSIRT
(*5) Tim Gulih JabarProv-CSIRT Bidang Infrastruktur
(*6) Tim Gulih JabarProv-CSIRT Bidang Aptika