

Formulir Penanganan Insiden

1. Informasi Umum	
Nama Lengkap	
Jabatan	
Instansi	
Nomor Telepon/HP	
Alamat Email	
Informasi Tambahan	

2. Deskripsi Insiden	
2.1 Jenis Insiden	
<input type="checkbox"/> Web Defacement	<input type="checkbox"/> Malware Infection
<input type="checkbox"/> Account Compromise	<input type="checkbox"/> Network Penetration
<input type="checkbox"/> Data Theft	
<input type="checkbox"/> Service Disruption	
<input type="checkbox"/> Unauthorized System Access	
<input type="checkbox"/> Denial of Services	
Penjelasan Insiden :	

2.2 Dampak dari Insiden

- Berhenti/hilangnya layanan
- Berhenti/hilangnya produktivitas
- Hilangnya Reputasi
- Berkurang/hilangnya pendapatan
- Pengubahan tidak sah dari data/informasi
- Lainnya :

Penjelasan dampak dari insiden :

2.3 Sensitivitas dari informasi yang terkena dampak insiden

- | | |
|---|--|
| <input type="checkbox"/> Data/Info Rahasia/Sensitive | <input type="checkbox"/> Informasi Identitas Personil |
| <input type="checkbox"/> Data/Info Non-Sensitive | <input type="checkbox"/> Data/Info tentang HAKI |
| <input type="checkbox"/> Data/Info yang disediakan untuk publik | <input type="checkbox"/> Data/Info tentang critical infrastructure/
key resources |
| <input type="checkbox"/> Data/Info keuangan | <input type="checkbox"/> Lainnya : |

Data dienkripsi	YA / TIDAK
Besarnya data/info yang terkena insiden (Ukuran file, Jumlah Record)	
Informasi Tambahan :	
2.4 Sistem yang terkena insiden	
Alamat IP dari sistem	
Nama Domain dari sistem	
Fungsi dari sistem (Web Server, Domain Controller)	
Sistem Operasi dari sistem (version, service pack, configuration)	
Level Patching dari sistem (latest patches loaded)	
Perangkat lunak security pada sistem (anti-virus, anti-spyware, firewall)	

Lokasi Fisik dari sistem (propinsi, kota, gedung, ruang, meja/rak/lemari)	
Informasi Tambahan :	

3. Timeline dari insiden	
Tanggal dan waktu kejadian pertama kali terdeteksi, ditemukan, atau diberitahu tentang insiden itu:	
Tanggal dan waktu saat kejadian yang sebenarnya terjadi: (perkiraan, jika tanggal dan waktu yang tepat tidak diketahui):	
Tanggal dan waktu ketika insiden itu ditangani atau ketika semua sistem/fungsi telah dipulihkan (menggunakan	

tanggal dan waktu terakhir):	
Tenggang waktu antara penemuan dan kejadian : Tenggang waktu antara penemuan dan pemulihan :	
Keterangan tambahan:	

4. Pengguna yang terdampak

Nama dan jenis pekerjaan pengguna:	
Level hak akses dari pengguna: (regular user, domain administrator, root)	
Keterangan tambahan:	

5. Pemulihan dari insiden

Tindakan yang dilakukan untuk mengidentifikasi sumber daya yang terkena dampak:

Tindakan yang dilakukan untuk memulihkan insiden:

Rencana tindakan untuk mencegah berulangnya insiden:

Keterangan tambahan:

Pembuat Laporan Insiden

Perespon Insiden

()

()