

## *Forma e raportimit të incidentit kibernetik*

### Sekcioni 1: Të dhëna e kontaktit të reportuesit

Emër Mbiemër:		Pozicioni i punës:	
Institucioni:		E-mail:	
Tel:		Cel:	

### Të dhënat e infrastrukturës së prekur nga sulmi

Emri i sistemit/rrjetit:

Lloji i infrastrukturës së informacionit:

Kritike

E rëndësishme

### Lloji i asistencës që kërkoni nga AKCESK

<input type="checkbox"/> Vetëm raportim	<input type="checkbox"/> Trajtim	<input type="checkbox"/> Rekomandime
---	----------------------------------	--------------------------------------

### Sekcioni 2 : Detajet e incidentit

#### Identifikimi i incidentit

<input type="checkbox"/> Alarm i pajisjes	<input type="checkbox"/> Analiza e log-eve	<input type="checkbox"/> Help Desk
<input type="checkbox"/> Njoftim nga përdoruesi	<input type="checkbox"/> Njoftim nga Endpoint Security Software	

Tjetër: \_\_\_\_\_

#### Statusi aktual i incidentit

<input type="checkbox"/> Po ndodh	<input type="checkbox"/> Nën kontroll	<input type="checkbox"/> Ka ndodhur
-----------------------------------	---------------------------------------	-------------------------------------

#### Kategoria e incidentit

<input type="checkbox"/> Compromised information	<input type="checkbox"/> Compromised asset	<input type="checkbox"/> Unauthorised access	<input type="checkbox"/> Malicious Code
<input type="checkbox"/> Intrusions against networks	<input type="checkbox"/> Theft or Loss	<input type="checkbox"/> Scans / Probes / Attempted Access	
<input type="checkbox"/> Phishing or Social Engineering	<input type="checkbox"/> Policy violations	<input type="checkbox"/> Theft/loss of assets	
<input type="checkbox"/> Unauthorised release of or disclosure of information	<input type="checkbox"/> Tjetër		

#### Të dhënat e incidentit

Burimi IP/Port:		Destinacioni IP/Port:	
Të dhënat e përfshira në incident a ishin të enkriptuara:	<input type="checkbox"/> Po <input type="checkbox"/> Jo		
<b>Kohëzgjatja e incidentit</b>			
Nga data/ora:		Në datën/orën:	
<b>Impakti i incidentit</b>			
Numri i përdoruesve të prekur:			
Koha që sistemi është jashtë shërbimit:			
Dëmi i sistemit:			
Humbja financiare:			
Ka apo jo humbje të dhënash:			
<b>Ju lutem përfshini 5-10 rreshta të “time-stamped logs” në “plain ASCII”</b>			
<b>Ju lutem bëni një përshkrim të shkurtër të incidentit dhe pasojave</b>			