Anexa nr. 2

Instrucţiuni de completare a formularului de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

Formularul va fi completat pentru fiecare incident cu impact semnificativ care a avut loc în anul 2012.
Un incident cu impact semnificativ reprezintă acel incident care afectează un număr mai mare de 5.000 de conexiuni timp de cel puţin o oră.

Tabel 1. Descrierea câmpurilor formularului de raportare

1. Furnizor	
Se va completa cu denumirea furnizorului care trimite raportul către ANCOM.	
2. Data şi ora	
2.1 Data şi ora la care s-a produs incidentul	Se vor completa data şi ora la care s-a produs incidentul, respectiv la care s-a descoperit incidentul.
2.2 Data şi ora la care s-a descoperit incidentul	
3. Impactul incidentului şi tipul cauzei	
3.1 Servicii afectate de incident:	
Se va bifa serviciul/serviciile a căror furnizare a fost afectată de incident.	
3.2 Parametrii de impact:	
Numărul de conexiuni afectate de incident per serviciu	Se va specifica numărul total de conexiuni afectate de incident pentru fiecare serviciu afectat în parte. O conexiune reprezintă: - în cazul serviciilor de acces la internet la puncte fixe: o conexiune de acces la internet; - în cazul serviciilor de transmisiuni de date la puncte fixe: o conexiune de acces la servicii de transmisiuni de date; - în cazul serviciilor de telefonie la punct fix: o linie telefonică alocată unui abonat de către un furnizor prin intermediul propriei reţele publice fixe pe care o operează sau prin reţeaua publică fixă a unui terţ; un abonat poate avea alocate una sau mai multe linii de acces; - în cazul serviciilor de telefonie, acces la internet şi transmisiuni de date furnizate prin intermediul reţelelor radio mobile celulare: o cartelă SIM activă; - în cazul serviciilor de retransmisie a programelor media audiovizuale liniare: un abonat. În cazul serviciilor furnizate prin intermediul unor reţele publice mobile terestre, furnizorul va estima numărul posibililor utilizatori afectaţi ţinând cont de utilizarea normală a sistemelor afectate (exemplu: dacă o staţie de bază care deserveşte în medie 1000 de utilizatori/SIM pe oră este inactivă timp de o oră, impactul acestui incident va fi estimat la 1000 de conexiuni).
Resursele/echipamentele afectate	Se vor specifica resursele/echipamentele afectate de incident. Ca şi exemplu, este prezentată în continuare o listă de resurse ce pot fi afectate: - staţii de bază pentru PLMN (BSC, BTS, RNC, NodeB etc.):

	- reţea locală (cabluri de cupru, fibră etc.); - cabinete stradale; - echipamente de comutare sau rutare (comutatoare de reţea, routere, multiplexoare etc.) - noduri de transmisiuni; - centre de comutaţie; - centre de mesaje; - registre de utilizatori (HLR, VLR, AuC, Home Subscriber Server etc.); - backbone; - interconectări; - echipamente pentru alimentarea de rezervă cu energie electrică (baterii, generatoare); - sisteme de alimentare cu energie electrică.
Durata incidentului	Se va specifica intervalul de timp dintre momentul în care serviciul începe să se degradeze sau s-a întrerupt până în momentul în care acesta este restabilit la parametrii iniţiali. Timpul va fi exprimat în ore (ex: 2h şi 45 de minute va fi reprezentat în 2,75 h).
Aria/răspândirea geografică	Se va specifica regiunea geografică afectată de incident (ex: regiunea, judeţele, localităţile).
Impactul asupra apelurilor de urgenţă	Se va specifica modul în care au fost afectate comunicaţiile către Sistemul naţional unic pentru apeluri de urgenţă.
3.3 Descrierea incidentului:	
Se va completa cu orice informaţii şi detalii disponibile privind apariţia, dezvoltarea, impactul incidentului şi modalitatea în care au fost afectate resursele/echipamentele.	
3.4 Tipul cauzei incidentului:	
Se va bifa cauza/cauzele incidentului: eroare umană, eroare de sistem, fenomen natural, acţiune rău intenţionată şi cauză externă/parte terţă. De obicei, categoria cauză externă/parte terţă poate fi corelată cu una din celelalte 4 cauze (de exemplu: în cazul unui cablu de fibră optică distrus în urma unor lucrări de construcţie, cauzele incidentului vor fi eroare umană şi cauză externă/parte terţă). Unele incidente pot avea o cauză iniţială şi una subsecventă, incidentele apărând în urma unei succesiuni de evenimente sau factori (exemplu: în cazul unui incident datorat unei alimentări defectuoase cu energie electrică – suprasarcină care produce o defectare a unui echipament al furnizorului, cauza iniţială este eroare de sistem al unui echipament al furnizorului de utilităţi şi cauză externă/parte terţă, iar cauza subsecventă este eroare de sistem – defecţiune hardware al unui echipament de comunicaţii electronice). În acest caz, furnizorul va bifa cauza iniţială.	
3.5 Mai multe informaţii despre cauza incidentului:	
Câmpul va cuprinde descrierea detaliată a cauzei incidentului, inclusiv vulnerabilităţile exploatate. În cazul incidentelor apărute în urma unei succesiuni de evenimente, furnizorul va oferi atât detalii privind cauza iniţială, cât şi despre cauza/cauzele subsecvente.	
4. Alte informaţii despre incident	
4.1 Acţiuni de răspuns la incident (inclusiv momentul când au fost luate):	
Câmpul va cuprinde descrierea detaliată a: - măsurilor de securitate implementate până la momentul producerii incidentului în vederea minimizării riscului incidentului; - acţiunilor întreprinse şi a măsurilor adoptate pentru a restabili serviciul la parametrii iniţiali în cazul în care incidentul afectează doar calitatea serviciului (nu există întrerupere în furnizarea serviciului); - acţiunilor întreprinse şi a măsurilor adoptate pentru a aduce serviciul la un nivel acceptabil, precum şi pentru a restabili serviciul la parametrii iniţiali în cazul întreruperii furnizării serviciului, inclusiv momentele de timp în care au fost acestea realizate.	
4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):	

Câmpul va cuprinde descrierea detaliată a acţiunilor realizate pentru a minimiza nivelul de risc şi pentru a preîntâmpina reapariţia incidentului (ex: revizuire măsuri de securitate şi proceduri, renegociere SLA-uri, instruiri de personal, achiziţie de echipamente sau sisteme de backup etc), precum şi momentul când au fost luate sau când vor fi luate aceste măsuri.
4.3 Alţi furnizori de reţele şi servicii de comunicaţii electronice afectaţi:
Acest câmp se completează cu detalii despre furnizorul şi resursele/serviciile acestuia afectate de incidentul în cauză, inclusiv cazurile în care furnizori din alte state membre ale Uniunii Europene au fost afectaţi.
4.4 Alte observaţii:
Acest câmp se completează cu orice alte detalii sau observaţii care nu au fost incluse în câmpurile de mai sus.