Anexa nr. 2

FORMULAR DE RAPORTARE
a incidentelor cu impact semnificativ asupra reţelelor şi serviciilor de comunicaţii electronice (disponibilitate, confidenţialitate, integritate sau autenticitate)

1. Furnizor: .....

2. Data şi ora:

- Data şi ora la care s-a produs incidentul — data: ..... ora: .....;
- Data şi ora la care s-a descoperit incidentul — data: ..... ora: .....;

3. Dimensiunea afectată a securității:

☐ disponibilitate;
☐ autenticitate;
☐ integritate;
☐ confidențialitate.

4. Incidentul este repetitiv:

☐ Da (specificați data ultimei apariții): .....;
☐ Nu.

5. Pragurile depășite:

☐ Incidentul a afectat mai mult de 5.000 de utilizatori timp de cel puțin 60 de minute sau a fost depășit pragul de 500.000 de ore-utilizator.
☐ Incidentul a afectat direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112.
☐ Incidentul a avut impact transfrontalier.
☐ Incidentul a afectat securitatea rețelelor și serviciilor altui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și i-a cauzat acestuia un incident care are un impact semnificativ, în măsura în care această situație este cunoscută.

6. Impactul incidentului:

- numărul de utilizatori afectați pentru fiecare serviciu: .....;
- durata incidentului (minute): .....;
- aria/răspândirea geografică:
  - numărul județelor afectate: .....;
  - denumirea județelor afectate: ..... .

7. Descrierea incidentului: .....

8. Acțiunile de răspuns: .....

9. Măsurile luate sau planificate pentru a împiedica producerea unui incident similar, inclusiv momentul când acestea au fost/vor fi luate, precum şi lecțiile învățate: .....

10. Alți furnizori de reţele şi servicii de comunicaţii electronice afectați:

☐ Da (specificați numele furnizorului/furnizorilor.): .....;
☐ Nu.

11. Persoana de contact: .....

Anexa nr. 3

INSTRUCȚIUNI DE COMPLETARE
a formularului de raportare a incidentelor cu impact semnificativ asupra reţelelor și serviciilor de comunicații electronice

1. Furnizor	
Se va completa cu denumirea furnizorului care trimite raportul către Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM).	
2. Data şi ora	
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. Formatul de introducere a datei va fi de tipul zz.ll.aaaa.
Data şi ora la care s-a descoperit incidentul.	
3. Dimensiunea afectată a securității	
Se va bifa dimensiunea securității care a fost afectată de incident (disponibilitatea, autenticitatea, integritatea sau confidențialitatea). Cele patru opțiuni au în vedere noua definiție a securității reţelelor şi serviciilor – „capacitatea rețelelor și serviciilor de comunicații electronice de a rezista, la un anumit nivel de încredere, oricărei acțiuni care afectează disponibilitatea, autenticitatea, integritatea sau confidențialitatea acestor rețele și servicii, a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de rețelele ori serviciile de comunicații electronice respective sau accesibile prin intermediul acestora.”	
4. Incidentul este repetitiv	
Se va bifa dacă un incident este repetitiv sau nu. În cazul în care este repetitiv se va/vor specifica data/datele (de tipul zz.ll.aaaa) precedentelor apariții. Un incident repetitiv se definește ca acel incident de securitate care are un impact semnificativ şi care cumulează următoarele 3 caracteristici: a) afectează aceleași resurse; b) are aceeași cauză; c) a mai fost raportat în precedentele 12 luni.	
5. Pragurile depășite	
Conform obligațiilor de raportare a incidentelor, acestea vor fi notificate în situația depășirii unuia dintre pragurile următoare, indiferent dacă acesta este cantitativ sau calitativ. Se va bifa una sau mai multe dintre opțiunile următoare: ☐ Incidentul a afectat mai mult de 5.000 de utilizatori timp de cel puțin 60 de minute sau a fost depășit pragul de 500.000 de ore-utilizator. Incidentele care afectează disponibilitatea sunt raportabile folosind pragul de număr de utilizatori şi timp (mai mult de 5.000 de utilizatori timp de cel puțin 60 de minute sau 500.000 de ore-utilizator), pe când cele care afectează autenticitatea, integritatea sau confidențialitatea sunt raportabile folosind doar pragul de număr de utilizatori (mai mult de 5.000 de utilizatori), indiferent de durata incidentului. Pragul ore–utilizator se calculează folosind formula: Ore-utilizator = (Număr de utilizatori afectați x durată incident, exprimată în minute) / 60	

☐ Incidentul a afectat direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112 - în situația în care un incident împiedică rutarea traficului către 112, acesta se va notifica. Pentru clarificare, incidentele care afectează serviciul de comunicații de voce și, implicit, apelarea către numărul unic pentru apeluri de urgență 112 nu vor fi raportate conform acestui prag, ci conform pragului cantitativ.

☐ Incidentul a avut impact transfrontalier – în situația în care un incident afectează utilizatori ai unor furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului din afara granițelor României, acesta va fi notificat.

☐ Incidentul a afectat securitatea rețelelor și serviciilor altui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și i-a cauzat acestuia un incident care are un impact semnificativ, în măsura în care această situație este cunoscută – în situația în care un incident din rețeaua proprie afectează un furnizor partener și îi provoacă acestuia un incident care are un impact semnificativ, acest incident va fi notificat, indiferent dacă este atins sau nu un prag cantitativ în rețeaua proprie.

6. Impactul incidentului	
Numărul de utilizatori afectați de incident	Se va specifica numărul de utilizatori afectați de incident pe fiecare tip de serviciu afectat în parte. NOTĂ: În cazul în care incidentul afectează alte dimensiuni ale securității, în afară de disponibilitate, este necesară specificarea numărului de utilizatori, precum şi o descriere a ce anume a fost afectat.
Durata incidentului	Se va specifica intervalul de timp dintre momentul în care serviciul începe să se degradeze sau s-a întrerupt și momentul în care acesta este restabilit la parametrii inițiali. Timpul va fi exprimat în minute. În situația unui incident ce afectează autenticitatea, integritatea sau confidențialitatea, durata va fi măsurată ca intervalul de timp dintre ora (estimată) a producerii breșei de securitate şi ora rezolvării sau încheierii acesteia.
Aria/răspândirea geografică	Se vor specifica informațiile aferente celor două elemente: - numărul județelor afectate: …….. - denumirea județelor afectate: …….

7. Descrierea incidentului
Se va completa cu orice informații şi detalii relevante disponibile. Descrierea va fi sub formă de text şi va cuprinde în mod obligatoriu cel puțin următoarele elemente: succesiunea evenimentelor care au dus la incident, tehnologia/protocolul afectată/afectat de incident, cauza incidentului (atât cauza principală, cât şi cea subsecventă, incluzând şi cauzele tehnice), resursele afectate de incident, localizarea echipamentelor afectate în cadrul rețelei şi nivelul la care componentele au fost afectate.

8. Acțiunile de răspuns

Câmpul va cuprinde măsurile de securitate implementate până la momentul producerii incidentului și descrierea detaliată a acțiunilor de răspuns, inclusiv momentele în care au fost acestea realizate. Spre exemplu, se vor detalia acțiunile întreprinse pentru a aduce serviciul la un nivel acceptabil, precum şi pentru a restabili serviciul la parametrii inițiali, în cazul afectării disponibilității, acțiunile întreprinse în ceea ce privește limitarea pierderii suplimentare a datelor, evaluarea pierderilor survenite prin colectarea faptelor și evaluarea riscurilor, inclusiv a potențialelor prejudicii aduse persoanelor afectate, în cazul afectării autenticității, integrității sau confidențialității. Se vor menționa alte autorități care au fost contactate și acțiunile de informare a persoanelor implicate în incident, dacă este cazul.
9. Măsurile luate sau planificate pentru a împiedica producerea unui incident similar, inclusiv momentul când acestea au fost/vor fi luate, precum şi lecțiile învățate
Câmpul va cuprinde descrierea detaliată a acțiunilor realizate pentru a minimiza nivelul de risc şi pentru a preîntâmpina reapariția incidentului (de exemplu, revizuire măsuri de securitate şi proceduri, renegociere SLA-uri, instruiri de personal, achiziție de echipamente sau sisteme de backup etc.), precum şi momentul când au fost luate sau când vor fi luate aceste măsuri. Acest câmp va conține și informații despre lecțiile învățate - aceasta presupune realizarea unui bilanț al incidentului, ajungerea la sursa problemei (root cause), cum și de ce s-a întâmplat, evaluarea a cât de bine a funcționat planul de răspuns la incident pentru a rezolva problema și identificarea îmbunătățirilor care trebuie făcute.
10. Alți furnizori de reţele şi servicii de comunicaţii electronice afectați
Se va bifa una dintre cele 2 opțiuni. În situația în care sunt afectați și alți furnizori, se vor specifica denumirile furnizorilor afectați de incidentul în cauză.
11. Persoana de contact
Se vor indica datele de contact ale persoanei responsabile (nume, prenume, număr telefon de contact, e-mail) cu furnizarea clarificărilor de natură tehnică, în cazul în care va fi nevoie.