AGENŢIA NAŢIONALĂ PENTRU REGLEMENTARE ÎN COMUNICAŢII ELECTRONICE ŞI TEHNOLOGIA INFORMAŢIEI A REPUBLICII MOLDOVA

НАЦИОНАЛЬНОЕ АГЕНТСТВО ПО РЕГУЛИРОВАНИЮ В ОБЛАСТИ ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ МОЛДОВА

CONSILIUL DE ADMINISTRAŢIE

H O T Ă R Â R E

mun. Chişinău

din _____ **Nr. _____**

privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra acestora

Întru respectarea Acordului de Asociere între Republica Moldova şi Uniunea Europeană pe de o parte, şi Uniunea Europeană şi Comunitatea Europeană a Energiei Atomice şi statele membre ale acestora, pe de altă parte, ratificat prin Legea nr.112 din 02.07.2014 *(Monitorul Oficial, 2014, nr.185-199, art.442);*

În temeiul art. 8 alin. (6) lit. e), art. 20, alin. (2) lit. e), art. 23, alin. (13) lit. o) din Legea comunicaţiilor electronice nr.241-XVI din 15 noiembrie 2007 (*Monitorul Oficial al Republicii Moldova, 2008, nr. 51-54, art. 155),* cu modificările şi completările ulterioare, pct. 14 şi pct. 15 lit. b) din Regulamentul Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei, aprobat prin Hotărârea Guvernului Republicii Moldova nr. 905 din 28 iulie 2008 *(Monitorul Oficial al Republicii Moldova, 2008, nr. 143-144, art. 917);*

În conformitate cu pct. 29 din Regulamentul privind regimul de autorizare generală şi eliberare a licenţelor de utilizare a resurselor limitate pentru furnizarea reţelelor şi serviciilor publice de comunicaţii electronice aprobat prin Hotărârea Consiliului de Administraţie al Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei nr. 57 din 21.12.2010 *(Monitorul Oficial al Republicii Moldova, 2011, nr.22-24,art.127),* cu modificările și completările ulterioare, Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directivă-cadru) (JO L 108, 24.4.2002, p. 33);

Întru implementarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărârea de Guvern cu nr. 811 din 29 octombrie 2015 *(Monitorul Oficial al Republicii Moldova, 2015, nr. 306-310, art. 905);*

În scopul garantării continuităţii serviciilor de comunicaţii electronice furnizate prin intermediul reţelelor publice de comunicaţii electronice, Consiliul de Administraţie

HOTĂRĂŞTE:

1. Se stabilesc măsurile minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, conform Anexei.

2. Furnizorii de rețele și servicii publice de comunicații electronice au obligaţia să desemneze o persoană/persoane responsabile de raportarea incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice și să transmită către Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei (ANRCETI) datele de contact ale acestui/acestora, în termen de 5 zile de la intrarea în vigoare a prezentei hotărâri, precum şi orice modificare a acestor date, în termen de 5 zile de la survenirea modificărilor.

3. Furnizorii de reţele şi servicii publice de comunicaţii electronice vor întreprinde măsurile necesare privind implementarea prezentei Hotărâri, în termen de 3 luni de la intrarea în vigoare a acesteia.

4. Anual, către data de 31 ianuarie, furnizorii de reţele și servicii publice de comunicaţii electronice au obligaţia de a transmite către ANRCETI notificarea anuală generalizată privind existenţa incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, completând formularul-tip de raportare prevăzut în Anexa 1, cu respectarea instrucţiunilor de completare specificate în Anexa 2 la prezenta hotărâre.

5. Anual, către data de 1 martie, ANRCETI întocmește și publică pe pagina sa de Internet un raport de sinteză privind notificările primite și măsurile luate de către furnizorii de reţele și servicii publice de comunicaţii electronice în conformitate cu prezenta Hotărâre.

6. Prezenta Hotărâre se publică în Monitorul Oficial al Republicii Moldova.

Preşedintele
Consiliului de Administraţie **Grigore VARANIȚA**

Membrii
Consiliului de Administraţie **Corneliu JALOBA**

Iurie URSU

Anexă
la Hotărârea Consiliului de
Administrație al ANRCETI
nr. din

Măsurile minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor și serviciilor publice de comunicaţii electronice

I. DISPOZIȚII GENERALE

1. Prezenta Hotărâre este elaborată de către Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei (ANRCETI).

2. Prezenta Hotărâre are ca obiect stabilirea măsurilor minime care trebuie luate de furnizorii de reţele şi servicii publice de comunicaţii electronice în vederea asigurării unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, circumstanţele, formatul şi procedurile aplicabile notificării privind încălcarea securităţii sau pierderea integrităţii cu un impact semnificativ asupra furnizării reţelelor şi serviciilor publice de comunicaţii electronice.

3. În înţelesul prezentei Hotărâri, următorii termeni se definesc astfel:

1) *securitatea şi integritatea reţelei şi serviciilor de comunicaţii electronice* – capacitatea unei reţele sau a unui serviciu public de comunicaţii electronice de a rezista evenimentelor, accidentale sau rău-intenţionate, care pot compromite sau afecta continuitatea furnizării reţelelor şi serviciilor publice de comunicaţii electronice la un nivel de performanţă echivalent cu cel anterior producerii evenimentului;

2) *incident* – un eveniment care poate afecta sau ameninţa, direct sau indirect, securitatea şi integritatea reţelei şi serviciilor publice de comunicaţii electronice (efectele cauzate de lucrările de întreţinere a reţelei, programate şi anunţate din timp utilizatorilor, nu sunt considerate incidente);

3) *incident cu impact semnificativ* – întreruperea pentru mai mult de 1 oră a furnizării serviciilor voce pentru cel puţin 10% din utilizatori Prepay, și/sau cel puţin 2% utilizatori cu abonament, sau 500 utilizatori corporativi. Această definiţie nu ia în calcul circumstanţele sezoniere care pot cauza degradarea nivelului de performanţă şi care nu depind de voinţa furnizorului de reţele şi servicii publice de comunicaţii electronice (ex. deconectările frecvente a energiei electrice în anumite perioade);

4) *măsuri de securitate* – mijloace (de natură administrativă, managerială, tehnică sau juridică) de management al riscurilor, incluzând politici, acţiuni, planuri, echipamente, facilităţi, proceduri, tehnici etc. menite să elimine ori să reducă riscurile privind securitatea şi integritatea reţelelor sau a serviciilor de comunicaţii electronice.

II. MĂSURILE MINIME DE SECURITATE

4. Furnizorii de reţele publice și/sau servicii publice de comunicaţii electronice, în continuare denumiți furnizori, au obligațiile după cum urmează:

1) să ia toate măsurile de securitate adecvate pentru a administra riscurile la adresa securităţii reţelelor şi serviciilor publice de comunicaţii electronice astfel încât să asigure un nivel de securitate corespunzător riscului identificat şi să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor şi reţelelor interconectate, având în vedere cele

mai noi tehnologii şi, acolo unde este cazul, de a colabora cu alţi furnizori pentru implementarea acestor măsuri;

2) să ia toate măsurile de securitate necesare pentru a administra riscurile la adresa integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, în scopul garantării integrităţii reţelelor şi al asigurării continuităţii furnizării serviciilor prin intermediul acestor reţele şi, acolo unde este cazul, de a colabora cu alţi furnizori pentru implementarea acestor măsuri.

5. Măsurile minime de securitate pe care trebuie să le stabilească şi să le implementeze furnizorii, astfel încât să îndeplinească obligaţia prevăzută la alin. 1) din pct.4 şi, după caz, cea prevăzută la alin. 2) din pct.4 vor viza cel puţin următoarele domenii:

1) politica de securitate şi managementul riscului;
2) securitatea resurselor umane;
3) securitatea şi integritatea reţelelor, facilităţilor asociate şi informaţiilor;
4) managementul operaţiunilor;
5) managementul incidentelor;
6) managementul continuităţii afacerii;
7) monitorizare, testare şi audit.

6. Furnizorii au obligaţia de a evalua şi, dacă este cazul, de a actualiza măsurile minime de securitate care vor viza domeniile identificate la pct. 5 ori de câte ori este necesar, însă cel puţin o dată la 12 luni.

7. Cu referință la domeniile identificate la pct. 5 furnizorii au obligaţia de a întreprinde măsurile minime de securitate după cum urmează.

8. Politica de securitate şi managementul riscului

Furnizorii au obligaţia:

1) să stabilească o politică de securitate adecvată;
2) să stabilească un management al riscului care:

a) să stabilească domeniul de aplicare, precum şi criteriile de bază necesare procesului de management al riscului (criteriul de evaluare a riscului, criteriul de stabilire a impactului, criteriul de acceptare a riscului);

b) să identifice riscurile, prin identificarea resurselor furnizorului în cauză, ameninţărilor, vulnerabilităţilor, măsurilor existente şi a consecinţelor pe care pierderea/încălcarea securităţii le-ar putea avea asupra resurselor;

c) să estimeze riscurile prin evaluarea impactului pe care îl poate avea concretizarea unei ameninţări care exploatează o vulnerabilitate a unei resurse şi prin evaluarea probabilităţii de apariţie a incidentelor;

d) să evalueze riscul;

e) să evalueze opţiunile de tratare a riscului, să selecteze măsuri pentru tratarea riscului cu fixarea obiectivelor acestor măsuri şi să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului;

3) să stabilească o structură adecvată a rolurilor şi responsabilităţilor în asigurarea securităţii şi integrităţii reţelelor şi serviciilor;

4) să stabilească o politică cu privire la cerinţele de securitate pentru achiziţionarea de produse şi servicii de la terţe părţi şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a produselor şi serviciilor (servicii IT, software, interconectare, baze de date, facilităţi asociate etc.).

9. Securitatea resurselor umane

Furnizorii au obligaţia:

1) să efectueze controale de verificare de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor în conformitate cu legile aplicabile, reglementările şi etica, proporţionale cu riscurile percepute;

2) să se asigure că personalul lor are cunoştinţe suficiente de securitate şi este instruit permanent cu privire la securitatea şi integritatea reţelelor şi serviciilor;

3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilităţi;

4) să stabilească un proces disciplinar pentru angajaţii care produc o încălcare a securităţii şi integrităţii reţelelor sau serviciilor de comunicaţii electronice.

10. Securitatea şi integritatea reţelelor, a facilităţilor asociate şi a informaţiilor

Furnizorii au obligaţia:

1) să stabilească o securitate fizică adecvată a reţelei şi a infrastructurii asociate (stabilirea şi menţinerea unor măsuri care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundaţiilor, cutremurelor, descărcărilor electrice, exploziilor, tulburărilor publice şi a altor forme de dezastre naturale, erorilor de transmisii de date, ale furnizorilor, sau utilizatorilor sau actelor de vandalism, furturilor, fraudărilor sau altor acte provocate intenţionat);

2) să stabilească o securitate adecvată a utilităţilor-suport, cum ar fi furnizarea de energie electrică în caz de perturbări sau întreruperi electrice, combustibil sau răcirea echipamentelor;

3) să stabilească măsuri de securitate adecvate pentru accesul (logic) la reţea şi la sistemele informatice (softwarelor, hardurilor, procedeelor de operare etc.);

4) să stabilească măsuri de securitate adecvate pentru a asigura protecţia reţelelor şi serviciilor de comunicaţii electronice împotriva codurilor cu potenţial dăunător, codurilor mobile neautorizate şi a atacurilor informatice, inclusiv DoS/DDoS (Refuzul, blocarea serviciului - Denial of Service/ Blocarea distribuită a serviciului - Distributed Denial of Service attacks).

11. *Managementul operaţiunilor*

Furnizorii au obligaţia:

1) să stabilească proceduri operaţionale şi responsabilităţi adecvate;

2) să stabilească proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice şi în software-urile de aplicaţii;

3) să stabilească proceduri de gestionare a resurselor astfel încât disponibilitatea şi starea acestora să fie verificată.

12. *Managementul incidentelor*

Furnizorii au obligaţia:

1) să stabilească procese şi proceduri pentru managementul incidentelor care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente şi escaladarea acestuia), inclusiv prin definirea rolurilor şi responsabilităţilor;

2) să stabilească un sistem de detectare a incidentelor;

3) să stabilească o procedură adecvată de raportare a incidentelor către ANRCETI, precum şi către alte autorităţi responsabile, şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori afectaţi, media, utilizatori, parteneri de afaceri etc.).

13. *Managementul continuităţii afacerii*

Furnizorii au obligaţia:

1) să stabilească o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor publice de comunicaţii electronice în situaţiile generate de perturbări grave ale funcţionării reţelei sau serviciului;

2) să deţină capabilităţi de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare.

14. Monitorizare, testare şi audit

Furnizorii au obligaţia:

1) să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem;

2) să stabilească politici pentru testarea, inclusiv prin exerciţii, a planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcţionării reţelei sau serviciului;

3) să stabilească politici pentru testarea echipamentelor, sistemelor şi software-lor, în special înainte de conectarea/punerea lor în funcţiune;

4) să stabilească o politică adecvată pentru evaluarea şi testarea securităţii tuturor resurselor (echipamente, sisteme şi software etc.);

5) să stabilească o politică pentru monitorizarea conformităţii şi pentru audit, cu un proces de raportare a conformităţii şi de rezolvare a deficienţelor constatate în timpul auditului.

III. NOTIFICAREA PRIVIND ÎNCĂLCAREA SECURITĂŢII SAU PIERDEREA INTEGRITĂŢII

15. Furnizorii au obligaţia să transmită la ANRCETI, o notificare privind existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice.

16. În aplicarea pct.15, furnizorii au obligaţia să transmită la ANRCETI o notificare iniţială, până cel târziu la ora 13.00 a zilei lucrătoare următoare celei în care a fost detectat incidentul cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice.

17. Notificarea iniţială prevăzută la pct.16 se transmite de către una dintre persoanele responsabile prevăzute pct. 2 al Hotărârii, ca înscris în format electronic la adresa de poştă electronica a ANRCETI: office@anrceti.md, şi va cuprinde cel puţin următoarele elemente:

1) ora descoperirii incidentului;

2) serviciile şi/sau reţelele care sunt afectate de incident;

3) estimarea ariei geografice afectate, a numărului de conexiuni afectate, precum şi a efectelor incidentului asupra furnizării reţelelor şi serviciilor de către alţi furnizori, pe piaţa naţională de comunicaţii electronice sau pe cea din alte state;

4) estimarea efectelor în ceea ce priveşte apelarea numerelor pentru serviciile de urgență (112 sau, după caz, 901, 902, 903, 904);

5) descrierea sumară a cauzelor care au provocat incidentul;

6) estimarea graficului de restabilire a furnizării reţelelor şi serviciilor publice de comunicaţii electronice în parametrii normali de funcţionare;

7) îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;

8) informaţiile oferite publicului cu privire la existenţa unui incident, modalitatea de comunicare şi ora la care au fost comunicate informaţiile, dacă este cazul;

9) alte aspecte/elemente care pot permite ANRCETI să decidă dacă informarea publicului privind incidentul este sau nu în interesul public;

10) datele de contact (nume, prenume, număr de telefon, număr de fax, adresă de poştă electronică) ale persoanei/persoanelor care poate/pot da mai multe informaţii privind incidentul.

18. Este considerată dată a transmiterii înscrisului în format electronic data confirmării primirii de către ANRCETI a acestui înscris. ANRCETI asigură, fără întârziere şi în mod automat, confirmarea primirii înscrisului în formă electronică transmis la adresa de poştă electronica office@anrceti.md.

19. În situaţia în care confirmarea primirii unui înscris în format electronic nu s-a realizat în condiţiile pct.18, este considerată dată a transmiterii data la care înscrisul în format electronic a fost trimis, în măsura în care această dată poate fi determinată cu certitudine.

20. În aplicarea pct.15, furnizorii au obligaţia să transmită la ANRCETI o notificare finală privind existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, în termen de două săptămâni de la detectarea acestuia, completând formularul-tip de raportare prevăzut în Anexa 1, cu respectarea instrucţiunilor de completare specificate în Anexa 2.

21. În cazul în care, la momentul transmiterii notificării finale prevăzute la pct. 20 furnizorii nu au disponibile toate informaţiile prevăzute în formularul-tip de raportare, aceştia au obligaţia să transmită o notificare suplimentară cu informaţiile respective, completând formularul-tip de raportare prevăzut în Anexa 2, imediat ce acestea sunt disponibile, dar nu mai târziu de 3 săptămâni de la detectarea incidentului cu impact semnificativ.

22. Notificarea finală şi notificarea suplimentară prevăzute la pct. 20 şi respectiv 21, se transmit la sediul ANRCETI, cu următoarele date de identificare:

bd. Ştefan cel Mare, 134, MD -2012, mun. Chişinău, Republica Moldova; tel.:+373 22251317, fax: +373 22222885, e-mail: office@anrceti.md, în unul dintre următoarele moduri:

1) prin depunere, personal sau de către un reprezentant legal al furnizorului, sub luare de semnătură;

2) printr-un serviciu poştal;

3) printr-un înscris în format electronic, căruia i s-a aplicat o semnătură digitală autentică, bazată pe un certificat al cheii publice, nesuspendat sau nerevocat la momentul respectiv.

23. Este considerată data a transmiterii notificării, după caz, data înscrierii acesteia în Registrul general al corespondenţei de intrare al ANRCETI, denumit în continuare Registrul corespondenţei, data confirmării primirii la sediul ANRCETI a notificării prin serviciul de trimitere poştală recomandată cu confirmare de primire sau data confirmării primirii înscrisului în formă electronică.

24. Formularul-tip de raportare prevăzut la pct. 20 poate fi obţinut de la sediul ANRCETI, sau de pe pagina de Internet a ANRCETI.

25. Ca urmare a primirii notificării iniţiale prevăzute la pct. 16 şi atunci când consideră că este în interesul public, ANRCETI poate informa publicul cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, prin intermediul paginii de Internet a ANRCETI, sau poate solicita furnizorului să informeze publicul în acest sens.

26. La solicitarea ANRCETI, furnizorul are obligaţia să asigure informarea publicului cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi

integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, cel puţin prin una dintre următoarele modalităţi:

1) prin intermediul unei secţiuni speciale pe propria pagină de Internet;
2) prin canalul propriu de televiziune;
3) prin intermediul poştei electronice;
4) prin intermediul serviciului de mesagerie scurtă;
5) prin mass-media.

27. În cazul în care ANRCETI nu a stabilit prin solicitarea prevăzută la pct. 26 modalităţile şi condiţiile de informare a publicului, furnizorul va realiza informarea publicului cel puţin prin una dintre modalităţile prevăzute la pct. 26.

28. La solicitarea ANRCETI, furnizorii au obligaţia să furnizeze informațiile necesare evaluării securității și/sau integrității serviciilor și rețelelor publice ale acestora, inclusiv a politicilor de securitate documentate.

29. ANRCETI are dreptul să solicite unui organism independent calificat sau unei autorități naționale competente să efectueze un audit de securitate și să pună la dispoziția ANRCETI rezultatele acestuia. Costul auditului este suportat de către furnizor.

30. ANRCETI are dreptul de a investiga cazurile de nerespectare, precum și efectele asupra securității și integrității rețelelor publice de comunicații electronice.

FORMULAR DE RAPORTARE A INCIDENTELOR CARE AU AFECTAT SECURITATEA ŞI INTEGRITATEA REŢELELOR ŞI SERVICIILOR DE COMUNICAŢII ELECTRONICE		
1. Furnizor:		
2. Data şi ora		
2.1 Data şi ora la care s-a produs incidentul	Data:	Ora:
2.2 Data şi ora la care s-a descoperit incidentul	Data:	Ora:
3. Impactul incidentului şi tipul cauzei		
3.1 Serviciul/serviciile afectate:		**Numărul de conexiuni afectate:**
□ ***Servicii publice de telefonie:***		
□ *Servicii de telefonie furnizate prin intermediul reţelelor publice fixe*		
□ *Servicii de telefonie furnizate prin intermediul reţelelor publice mobile terestre*		
□ *Servicii de telefonie furnizate prin intermediul reţelelor publice cu transmisie prin satelit*		
□ *Servicii de transport apeluri*		
□ ***Servicii de linii închiriate***		
□ ***Servicii de transmisiuni de date (inclusiv VPN):***		
□ *La puncte fixe*		
□ *Fix-mobil*		
□ *SMS (numai în cazul reţelelor celulare)*		
□ *Mobil (inclusiv MVNO)*		
□ ***Servicii de acces la Internet:***		
□ *Dial-up (numai pentru bucla locală)*		
□ *Conexiuni permanente la punct fix*		
□ *Conexiuni radio mobile (inclusiv MVNO)*		
□ ***Retransmisia serviciilor de programe media audiovizuale liniare către utilizatorii finali:***		
□ *Cu acces fix prin satelit (tip DTH)*		
□ *Cu acces mobil prin satelit (tip S-DAB/DVB-S)*		
□ *Terestre cu acces la punct fix tip CATV, DVB-C/Mx,* □ *IPTV etc.*		
□ *Terestre dedicate tip DVB-T/DVB-T2*		
□ *Radio Celulare Publice (tip Mobile TV)*		
□ *Alte servicii de comunicaţii electronice*		
□ *Servicii de radiocomunicaţii mobile profesionale*		
□ *Comunicaţii voce*		
□ *Mesagerie radio*		

☐ *Transmisii de date, telex*	
☐ *Localizare, poziţionare*	
☐ ***Alte tipuri de servicii***	
☐ *Servicii de comunicaţii electronice care permit servicii voce*	
☐ *Servicii de comunicaţii electronice care permit accesul la servicii de conţinut*	
☐ *Alte tipuri de servicii decât cele de mai sus*	
3.2 Parametrii de impact:	
Numărul total de conexiuni afectate de incident:	
Resursele/echipamentele afectate:	
Durata incidentului:	
Aria/răspândirea geografică:	
Impactul asupra apelurilor de urgenţă:	
3.3 Descrierea incidentului:	
3.4 Tipul cauzei incidentului:	
☐ Eroare umană	
☐ Eroare de sistem	
☐ Fenomen natural	
☐ Acţiune rău intenţionată	
☐ Cauză externă/parte terţă	
3.5 Mai multe informaţii despre cauza incidentului:	
4. Alte informaţii despre incident	
4.1 Acţiuni de răspuns la incident (inclusiv momentul când au fost luate):	
4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):	
4.3 Alţi furnizori de reţele şi servicii de comunicaţii electronice afectaţi:	
4.4 Alte observaţii:	

Anexa 2

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

1. Furnizor:	
Se va completa cu denumirea furnizorului care trimite raportul către ANRCETI	
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. Formatul de introducere a datei va fi de tipul zz.ll.aaaa.*
2.2 Data şi ora la care s-a descoperit incidentul	
3. Impactul incidentului şi tipul cauzei	
3.1 Serviciul/serviciile afectate:	

Se va/vor bifa serviciul/serviciile a cărui/căror furnizare a fost afectată de incident.

Câmpul „Numărul de conexiuni afectate" din dreptul fiecărui tip de serviciu se va completa corespunzător, fiecărui serviciu afectat în parte fiindu-i alocat numărul de conexiuni afectate de incident.

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 terestre: o cartelă SIM activă;
- în cazul serviciilor de retransmisie a programelor media audiovizuale liniare: o conexiune de retransmisie a programelor media audiovizuale.

În cazul serviciilor furnizate prin intermediul unor reţele publice mobile terestre, furnizorul va estima numărul de conexiuni afectate. Metoda de estimare a numărului de cartele SIM afectate de un incident este următoarea:

În momentul apariţiei unui incident se identifică celulele afectate.

Traficul total pierdut la nivelul tuturor celulelor afectate ($T_{pierdut}$) pe fiecare serviciu (voce şi date) se consideră a fi traficul înregistrat în săptămâna anterioară, în acelaşi interval de timp în care a avut loc incidentul, la nivelul acelor celule.

Traficul total înregistrat la nivelul reţelei ($T_{reţea}$) se consideră a fi suma traficului din toate celulele din reţea în intervalul de timp respectiv, în săptămâna anterioară.

Numărul de cartele SIM afectate se calculează astfel:

$$N_{cartele\ sim\ afectate} = N_{ds}\frac{T_{pierdut}}{T_{reţea}}$$

N_{ds} reprezintă numărul de cartele SIM active pe respectivul serviciu la nivelul furnizorului,

conform raportării în baza Hotărârii Consiliului de Administraţie al ANRCETI nr.33 din 2011 cu privire la aprobarea formularelor rapoartelor statistice pentru furnizorii de reţele şi/sau servicii publice de comunicaţii electronice. În calculul traficului, se are în vedere atât traficul originat, cât şi traficul terminat. Algoritmul propus se va aplica tuturor tipurilor de servicii la puncte mobile.	
3.2 Parametrii de impact:	
Numărul total de conexiuni afectate de incident:	*Se va specifica numărul total de conexiuni afectate de incident. Acest număr se va calcula ca sumă a numărului de conexiuni afectate pe fiecare tip de serviciu.*
Resursele/echipamentele afectate:	Se vor specifica resursele/echipamentele afectate de incident. Ca 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 minute.*
Aria/răspândirea geografică:	*Se va specifica regiunea geografică afectată de incident (de exemplu: municipiul, raionul, localităţile).*
Impactul asupra apelurilor de urgenţă:	*Se va specifica modul în care au fost afectate comunicaţiile către serviciile 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/vor 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 a unui echipament al furnizorului de utilităţi şi cauză externă/parte terţă, iar cauza subsecventă este eroare de sistem – defecţiune hardware a 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 (de exemplu: 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. De asemenea, se descrie modul de colaborare cu alţi furnizori în vederea soluţionării incidentului, inclusiv acţiunile comune de răspuns la incident.
4.4 Alte observaţii:
Acest câmp se completează cu orice alte detalii sau observaţii care nu au fost incluse în câmpurile de mai sus.