



CONSILIUL DE ADMINISTRAȚIE

HOTĂRÂRE

mun. Chișinău

din _

Nr. __

privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor publice de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra acestora

În temeiul art. 8 alin. (6) lit. e), art. 20, alin. (2) lit. e), art. 23, alin. (13) lit. o) din Legea comunicațiilor electronice nr.241-XVI din 15 noiembrie 2007 (*Monitorul Oficial al Republicii Moldova, 2008, nr. 51-54, art. 155*), cu modificările și completările ulterioare;

pct. 14 și pct. 15 lit. b) din Regulamentul Agenției Naționale pentru Reglementare în Comunicații Electronice și Tehnologia Informației, 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 și eliberare a licențelor de utilizare a resurselor limitate pentru furnizarea rețelelor și serviciilor publice de comunicații electronice aprobat prin Hotărârea Consiliului de Administrație al Agenției Naționale pentru Reglementare în Comunicații Electronice și Tehnologia Informației nr. 57 din 21.12.2010 (*Monitorul Oficial al Republicii Moldova, 2011, nr.22-24,art.127*), cu modificările și completările ulterioare;

Având în vedere prevederile art. 13a din 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, 24.04.2002, p. 33) astfel cum a fost modificată de Directiva 2009/140/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 (JO L 337, 18.12.2009, p. 37);

În scopul garantării continuității furnizării serviciilor de comunicații electronice prin intermediul rețelelor publice de comunicații electronice, Consiliul de Administrație

HOTĂRĂȘTE:

1. Se stabilesc măsurile minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor publice de comunicații electronice, conform Anexei.

2. Furnizorii de rețele și servicii publice de comunicații electronice au obligația să desemneze o persoană/persoane responsabile de raportarea incidentelor cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice și să transmită către Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI) datele de contact ale acestui/acestora, în termen de 15 zile de la

intrarea în vigoare a prezentei hotărâri, precum și orice modificare a acestor date, în termen de 5 zile de la survenirea modificărilor.

3. Furnizorii de rețele și servicii publice de comunicații electronice vor întreprinde măsurile necesare privind implementarea prezentei Hotărâri, în termen de 3 luni de la intrarea în vigoare a acesteia și vor comunica ANRCETI despre măsurile întreprinse.

4. Anual, către data de 31 ianuarie, furnizorii de rețele și servicii publice de comunicații electronice au obligația de a transmite către ANRCETI notificarea anuală generalizată privind existența incidentelor cu impact semnificativ asupra securității și integrității rețelelor și serviciilor publice de comunicații electronice, completând formularul-tip de raportare prevăzut în Anexa 1, cu respectarea instrucțiunilor 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 rețele și servicii publice de comunicații electronice în conformitate cu prezenta Hotărâre.

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

**Președintele
Consiliului de Administrație**

Grigore VARANIȚA

**Membrii
Consiliului de Administrație**

Corneliu JALOBĂ

Iurie URSU

Măsurile minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor publice de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra acestora

I. DISPOZIȚII GENERALE

1. Prezenta Hotărâre este elaborată de către Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI).

2. Prezenta Hotărâre are ca obiect stabilirea măsurilor minime care trebuie luate de furnizorii de rețele și servicii publice de comunicații electronice în vederea asigurării unui nivel adecvat al securității și integrității rețelelor și serviciilor publice de comunicații electronice, circumstanțele, formatul și procedurile aplicabile notificării privind încălcarea securității sau pierderea integrității cu un impact semnificativ asupra furnizării rețelelor și serviciilor publice de comunicații electronice.

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

1) *securitatea și integritatea rețelei și serviciilor de comunicații electronice* – capacitatea unei rețele sau a unui serviciu public de comunicații electronice de a rezista evenimentelor, accidentale sau rău-intenționate, care pot compromite sau afecta continuitatea furnizării rețelelor și serviciilor publice de comunicații electronice la un nivel de performanță echivalent cu cel anterior producerii evenimentului;

2) *incident* – un eveniment care poate afecta sau amenința, direct sau indirect, securitatea și integritatea rețelei și serviciilor publice de comunicații electronice (efectele cauzate de lucrările de întreținere a rețelei, programate și anunțate din timp utilizatorilor, nu sunt considerate incidente);

3) *incident cu impact semnificativ* – incident care afectează un număr mai mare de 500 de conexiuni, timp de cel puțin 60 de minute;

4) *măsurile de securitate* – mijloace (de natură administrativă, managerială, tehnică sau juridică) de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, tehnici etc. menite să elimine ori să reducă riscurile privind securitatea și integritatea rețelelor sau a serviciilor de comunicații electronice.

II. MĂSURILE TEHNICE ȘI ORGANIZATORICE

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

1) să ia toate măsurile de securitate adecvate pentru a administra riscurile la adresa securității rețelelor și serviciilor publice de comunicații electronice astfel încât să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, având în vedere cele mai noi tehnologii și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri;

2) să ia toate măsurile de securitate necesare pentru a administra riscurile la adresa integrității rețelelor și serviciilor publice de comunicații electronice, în scopul garantării integrității rețelelor și al asigurării continuității furnizării serviciilor prin intermediul acestor rețele și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.

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

- 1) politica de securitate și managementul riscului;
- 2) securitatea resurselor umane;
- 3) securitatea și integritatea rețelelor, a facilităților asociate și a informațiilor;
- 4) managementul operațiunilor;
- 5) managementul incidentelor;
- 6) managementul continuității afacerii;
- 7) monitorizare, testare și audit.

6. Furnizorii au obligația de a evalua și, 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 puțin o dată la 12 luni.

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

8. *Politica de securitate și managementul riscului*

Furnizorii au obligația:

- 1) să stabilească o politică de securitate adecvată;
- 2) să stabilească un management al riscului care:
 - a) să stabilească domeniul de aplicare, precum și 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, amenințărilor, vulnerabilităților, măsurilor existente și a consecințelor pe care pierderea/încălcarea securității le-ar putea avea asupra resurselor;
 - c) să estimeze riscurile prin evaluarea impactului pe care îl poate avea concretizarea unei amenințări care exploatează o vulnerabilitate a unei resurse și prin evaluarea probabilității de apariție a incidentelor;
 - d) să evalueze riscul;
 - e) să evalueze opțiunile de tratare a riscului, să selecteze măsuri pentru tratarea riscului cu fixarea obiectivelor acestor măsuri și să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului;
- 3) să stabilească o structură adecvată a rolurilor și responsabilităților în asigurarea securității și integrității rețelelor și serviciilor;
- 4) să stabilească o politică cu privire la cerințele de securitate pentru achiziționarea de produse și servicii de la terțe părți și pentru asigurarea întreținerii sau gestiunii de către terțe părți a produselor și serviciilor (servicii IT, software, interconectare, baze de date, facilități asociate etc).

9. *Securitatea resurselor umane*

Furnizorii au obligația:

- 1) să efectueze controale de verificare de fond a candidaților pentru angajare, a contractorilor și a terților în conformitate cu legile aplicabile, reglementări și etică, proporționale cu riscurile percepute;

- 2) să se asigure că personalul lor are cunoștințe suficiente de securitate și este instruit permanent cu privire la securitatea și integritatea rețelelor și serviciilor;
- 3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri și responsabilități;
- 4) să stabilească un proces disciplinar pentru angajații care produc o încălcare a securității și integrității rețelelor sau serviciilor de comunicații electronice.

10. *Securitatea și integritatea rețelelor, a facilităților asociate și a informațiilor*

Furnizorii au obligația:

- 1) să stabilească o securitate fizică adecvată a rețelei și a infrastructurii asociate (stabilirea și menținerea unor măsuri care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundațiilor, cutremurelor, descărcărilor electrice, exploziilor, tulburărilor publice și a altor forme de dezastre natural, erorilor de transmisii de date, ale furnizorilor, sau utilizatorilor sau actelor de vandalism, furturilor, fraudărilor sau alte acte provocate intenționat);
- 2) să stabilească o securitate adecvată a utilităților-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 rețea și la sistemele informatice (softwarelor, hardurilor, procedeele de operare etc.);
- 4) să stabilească măsuri de securitate adecvate pentru a asigura protecția rețelelor și serviciilor de comunicații electronice împotriva codurilor cu potențial dăunător, codurilor mobile neautorizate și a atacurilor informatice, inclusiv DoS/DDoS (Denial of Service/Distributed Denial of Service attacks).

11. *Managementul operațiunilor*

Furnizorii au obligația:

- 1) să stabilească proceduri operaționale și responsabilități adecvate;
- 2) să stabilească proceduri privind managementul schimbărilor efectuate în rețeaua de comunicații electronice și în software-urile de aplicații;
- 3) să stabilească proceduri de gestionare a resurselor astfel încât disponibilitatea și starea acestora să fie verificată.

12. *Managementul incidentelor*

Furnizorii au obligația:

- 1) să stabilească procese și proceduri pentru managementul incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente și escaladarea acestuia), inclusiv prin definirea rolurilor și responsabilităților;
- 2) să stabilească un sistem de detectare a incidentelor;
- 3) să stabilească o procedură adecvată de raportare a incidentelor către ANRCETI, precum și către alte autorități responsabile, și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori afectați, media, clienți, parteneri de afaceri etc.).

13. *Managementul continuității afacerii*

Furnizorii au obligația:

- 1) să stabilească o strategie pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în situațiile generate de perturbări grave ale funcționării rețelei sau serviciului;
- 2) să dețină capabilități de implementare a strategiei de continuitate și să stabilească planuri de continuitate și de recuperare.

14. Monitorizare, testare și audit

Furnizorii au obligația:

- 1) să stabilească politici de monitorizare a sistemelor, precum și politici privind jurnalele de sistem;
- 2) să stabilească politici pentru testarea, inclusiv prin exerciții, a planurilor de continuitate și de recuperare în cazul perturbărilor grave ale funcționării rețelei sau serviciului;
- 3) să stabilească politici pentru testarea echipamentelor, sistemelor și software-lor, în special înainte de conectarea/punerea lor în funcțiune;
- 4) să stabilească o politică adecvată pentru evaluarea și testarea securității tuturor resurselor (echipamente, sisteme și software etc.);
- 5) să stabilească o politică pentru monitorizarea conformității și pentru audit, cu un proces de raportare a conformității și de rezolvare a deficiențelor constatate în timpul auditului.

III. NOTIFICAREA PRIVIND ÎNCĂLCAREA SECURITĂȚII SAU PIERDEREA INTEGRITĂȚII

15. Furnizorii au obligația să transmită la ANRCETI, o notificare privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor publice de comunicații electronice.

16. În aplicarea pct.15, furnizorii au obligația să transmită la ANRCETI o notificare inițială, până cel târziu la ora 13.00 a zilei lucrătoare următoare celei în care a fost detectat incidentul cu impact semnificativ asupra securității și integrității rețelelor și serviciilor publice de comunicații electronice.

17. Notificarea inițială 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 poștă electronică a ANRCETI: office@anrceti.md, și va cuprinde cel puțin următoarele elemente:

- 1) ora descoperirii incidentului;
- 2) serviciile și/sau rețelele care sunt afectate de incident;
- 3) estimarea ariei geografice afectate, a numărului de conexiuni afectate, precum și a efectelor incidentului asupra furnizării rețelelor și serviciilor de către alți furnizori, pe piața națională de comunicații electronice sau pe cea din alte state;
- 4) estimarea efectelor în ceea ce privește 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 rețelelor și serviciilor publice de comunicații electronice în parametrii normali de funcționare;
- 7) îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;
- 8) informațiile oferite publicului cu privire la existența unui incident, modalitatea de comunicare și ora la care au fost comunicate informațiile, 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 poștă electronică) ale persoanei/persoanelor care poate/pot da mai multe informații 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 și în mod automat, confirmarea primirii înscrisului în formă electronică transmis la adresa de poștă electronică office@anrceti.md.

19. În situația în care confirmarea primirii unui înscris în format electronic nu s-a realizat în condițiile 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 obligația să transmită la ANRCETI o notificare finală privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor publice de comunicații electronice, în termen de două săptămâni de la detectarea acestuia, completând formularul-tip de raportare prevăzut în Anexa 1, cu respectarea instrucțiunilor 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 informațiile prevăzute în formularul-tip de raportare, aceștia au obligația să transmită o notificare suplimentară cu informațiile 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 și notificarea suplimentară prevăzute la pct. 20 și respectiv 21, se transmit la sediul ANRCETI, cu următoarele date de identificare:

bd. Ștefan cel Mare, 134, MD -2012, mun. Chișinău, 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 poștal;

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 corespondenței de intrare al ANRCETI, denumit în continuare Registrul corespondenței, data confirmării primirii la sediul ANRCETI a notificării prin serviciul de trimitere poștală recomandată cu confirmare de primire sau data confirmării primirii înscrisului în formă electronică.

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

25. Ca urmare a primirii notificării inițiale prevăzute la pct. 16 și atunci când consideră că este în interesul public, ANRCETI poate informa publicul cu privire la existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor publice de comunicații electronice, prin intermediul paginii de internet a ANRCETI, sau poate solicita furnizorului să informeze publicul în acest sens.

26. La solicitarea ANRCETI, furnizorul are obligația să asigure informarea publicului cu privire la existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice, cel puțin prin una dintre următoarele modalități:

1) prin intermediul unei secțiuni speciale pe propria pagină de internet;

2) prin canalul propriu de televiziune;

3) prin intermediul poștei 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 modalitățile și condițiile de informare a publicului, furnizorul va realiza informarea publicului cel puțin prin una dintre modalitățile prevăzute la pct. 26.

28. La solicitarea ANRCETI, furnizorii au obligația să furnizeze informațiile necesare evaluării securității și/sau integrității serviciilor și rețelelor 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.

FORMULAR DE RAPORTARE A INCIDENTELOR CARE AU AFECTAT SECURITATEA ȘI INTEGRITATEA REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE	
1. Furnizor:	
2. Data și ora	
2.1 Data și ora la care s-a produs incidentul	Data: _____ Ora: _____
2.2 Data și ora la care s-a descoperit incidentul	Data: _____ Ora: _____
3. Impactul incidentului și tipul cauzei	
3.1 Serviciul/serviciile afectate:	Numărul de conexiuni afectate:
☐ Servicii publice de telefonie:	
☐ Servicii de telefonie furnizate prin intermediul rețelelor publice fixe	
☐ Servicii de telefonie furnizate prin intermediul rețelelor publice mobile terestre	
☐ Servicii de telefonie furnizate prin intermediul rețelelor 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 rețelelor 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 comunicații electronice	
☐ Servicii de radiocomunicații mobile profesionale	
☐ Comunicații voce	
☐ Mesagerie radio	

☐ <i>Transmisii de date, telex</i>	
☐ <i>Localizare, poziționare</i>	
☐ Alte tipuri de servicii	
☐ <i>Servicii de comunicații electronice care permit servicii voce</i>	
☐ <i>Servicii de comunicații electronice care permit accesul la servicii de conținut</i>	
☐ <i>Alte tipuri de servicii decât cele de mai sus</i>	
3.2 Parametrii de impact:	
Numărul total de conexiuni afectate de incident:	
Resursele/echipamentele afectate:	
Durata incidentului:	
Aria/răspândirea geografică:	
Impactul asupra apelurilor de urgență:	
3.3 Descrierea incidentului:	
3.4 Tipul cauzei incidentului:	
☐ Eroare umană	
☐ Eroare de sistem	
☐ Fenomen natural	
☐ Acțiune rău intenționată	
☐ Cauză externă/parte terță	
3.5 Mai multe informații despre cauza incidentului:	
4. Alte informații despre incident	
4.1 Acțiuni 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 Alți furnizori de rețele și servicii de comunicații electronice afectați:	
4.4 Alte observații:	

**Instrucțiuni de completare a formularului de raportare a incidentelor
care au afectat securitatea și integritatea rețelelor și serviciilor
publice de comunicații electronice**

1. Furnizor:	
<i>Se va completa cu denumirea furnizorului care trimite raportul către ANRCETI</i>	
2. Data și ora	
2.1 Data și ora la care s-a produs incidentul	<i>Se vor completa data și 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.</i>
2.2 Data și ora la care s-a descoperit incidentul	
3. Impactul incidentului și tipul cauzei	
3.1 Serviciul/serviciile afectate:	
Se va/vor bifa serviciul/serviciile a căru/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 rețele publice fixe pe care o operează sau prin rețeaua publică fixă a unui terț; un abonat poate avea alocate una sau mai multe linii de acces; - în cazul serviciilor de telefonie, acces la internet și transmisiuni de date furnizate prin intermediul rețelelor 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 rețele 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 apariției unui incident se identifică celulele afectate. Traficul total pierdut la nivelul tuturor celulelor afectate ($T_{pierdut}$) pe fiecare serviciu (voce și date) se consideră a fi traficul înregistrat în săptămâna anterioară, în același interval de timp în care a avut loc incidentul, la nivelul acelor celule. Traficul total înregistrat la nivelul rețelei ($T_{rețea}$) se consideră a fi suma traficului din toate celulele din rețea în intervalul de timp respectiv, în săptămâna anterioară. Numărul de cartele SIM afectate se calculează astfel: $N_{cartele\ sim\ afectate} = N_{ds} \frac{T_{pierdut}}{T_{rețea}}$ N_{ds} reprezintă numărul de cartele SIM active pe respectivul serviciu la nivelul furnizorului,	

conform raportării în baza Hotărârii Consiliului de Administrație al ANRCETI nr.33 din 2011 cu privire la aprobarea formularelor rapoartelor statistice pentru furnizorii de rețele și/sau servicii publice de comunicații electronice. În calculul traficului, se are în vedere atât traficul originat, cât și 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:	<i>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.</i>
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: - stații de bază pentru PLMN (BSC, BTS, RNC, NodeB etc.); - rețea locală (cabluri de cupru, fibră etc.); - cabinete stradale; - echipamente de comutare sau rutare (comutatoare de rețea, routere; - multiplexoare etc.); - noduri de transmisiuni; - centre de comutație; - 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:	<i>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 inițiali. Timpul va fi exprimat în minute.</i>
Aria/răspândirea geografică:	<i>Se va specifica regiunea geografică afectată de incident (de exemplu: municipiul, raionul, localitățile).</i>
Impactul asupra apelurilor de urgență:	<i>Se va specifica modul în care au fost afectate comunicațiile către serviciile de urgență</i>
3.3 Descrierea incidentului:	
Se va completa cu orice informații și detalii disponibile privind apariția, dezvoltarea, impactul incidentului și 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, acțiune rău intenționată și cauză externă/parte terță. De obicei, categoria cauză externă/parte terță poate fi corelată cu una din celelalte 4 cauze (de exemplu: în cazul unui cablu de fibră optică distrus în urma unor lucrări de construcție, cauzele incidentului vor fi eroare umană și cauză externă/parte terță).	

Unele incidente pot avea o cauză inițială și 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 inițială este eroare de sistem a unui echipament al furnizorului de utilități și cauză externă/parte terță, iar cauza subsecventă este eroare de sistem – defecțiune hardware a unui echipament de comunicații electronice). În acest caz, furnizorul va bifa cauza inițială.
3.5 Mai multe informații despre cauza incidentului:
Câmpul va cuprinde descrierea detaliată a cauzei incidentului, inclusiv vulnerabilitățile exploatare. În cazul incidentelor apărute în urma unei succesiuni de evenimente, furnizorul va oferi atât detalii privind cauza inițială, cât și despre cauza/cauzele subsecvente.
4. Alte informații despre incident
4.1 Acțiuni 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; - acțiunilor întreprinse și a măsurilor adoptate pentru a restabili serviciul la parametrii inițiali în cazul în care incidentul afectează doar calitatea serviciului (nu există întrerupere în furnizarea serviciului); - - acțiunilor întreprinse și a măsurilor adoptate pentru a aduce serviciul la un nivel acceptabil, precum și pentru a restabili serviciul la parametrii inițiali 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 acțiunilor realizate pentru a minimiza nivelul de risc și pentru a preîntâmpina reapariția incidentului (de exemplu: revizuire măsuri de securitate și proceduri, renegociere SLA-uri, instruiți de personal, achiziție de echipamente sau sisteme de backup etc), precum și momentul când au fost luate sau când vor fi luate aceste măsuri.
4.3 Alți furnizori de rețele și servicii de comunicații electronice afectați:
Acest câmp se completează cu detalii despre furnizorul și resursele/serviciile acestuia afectate de incidentul în cauză, inclusiv cazurile în care furnizori din alte state membre ale Uniunii Europene au fost afectați. De asemenea, se descrie modul de colaborare cu alți furnizori în vederea soluționării incidentului, inclusiv acțiunile comune de răspuns la incident.
4.4 Alte observații:
Acest câmp se completează cu orice alte detalii sau observații care nu au fost incluse în câmpurile de mai sus.