



## CONSILIUL DE ADMINISTRAȚIE

### HOTĂRÂRE

mun. Chișinău

din \_\_\_\_\_

Nr. \_\_\_\_\_

#### **privind aprobarea Cerințelor referitoare la implementarea măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului**

În temeiul art. 8 alin. (6) lit. e), art. 9 alin. (1) lit. a), art. 10 alin. (1) lit. a), art. 20 alin.(2) lit. e), art. 21 alin. (4), art. 22, art. 25 alin. (16) pct. 9 și art. 64 alin. (1) lit. h) din Legea comunicațiilor electronice nr. 241/2007 (*republicată în Monitorul Oficial al Republicii Moldova, 2017, nr. 399-410, art. 679*), cu modificările și completările ulterioare,

În vederea implementării prevederilor art. 21 alin. (1) – (3) din Legea comunicațiilor electronice nr. 241/2007 (*republicată în Monitorul Oficial al Republicii Moldova, 2017, nr.399-410, art. 679*), cu modificările și completările ulterioare,

În scopul realizării acțiunii prevăzute la pct. 2 subpct.2.2 din Planul de acțiuni privind implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 aprobat prin Hotărârea Guvernului nr. 811/2015 (*Monitorul Oficial al Republicii Moldova, 2015, nr. 306-310, art. 905*), **Consiliul de Administrație**

### HOTĂRĂȘTE:

**1.** Se aprobă Cerințele referitoare la implementarea măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, conform anexei la prezenta Hotărâre.

**2.** Hotărârea se publică în Monitorul Oficial al Republicii Moldova și intră în vigoare la expirarea a trei luni de la data publicării.

**Președintele  
Consiliului de Administrație**

**Octavian RĂU**

**Membrii Consiliului de Administrație**

**Andrei MUNTEAN**

**Marian POCAZNOI**

## CERINȚE

### referitoare la implementarea măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului

#### I. DISPOZIȚII GENERALE

1. Cerințele referitoare la implementarea măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului (în continuare denumite prezentele Cerințe) stabilesc, în principal:

- 1) modalitățile de implementare a măsurilor minime de securitate;
- 2) circumstanțele, formatul și procedurile aplicate raportării incidentelor cu impact semnificativ asupra securității și integrității rețelelor publice de comunicații electronice și serviciilor de comunicații electronice accesibile publicului;
- 3) condițiile și modalitățile de informare a publicului cu privire la existența incidentelor menționate la subpunctul 1);
- 4) modalitățile de verificare a respectării cerințelor privind măsurile minime de securitate și evaluarea securității și integrității rețelelor și serviciilor de comunicații electronice.

2. În înțelesul prezentelor Cerințe, următorii termeni se definesc astfel:

1) *amenințare* – circumstanță sau eveniment care constituie un pericol potențial la adresa securității rețelei publice de comunicații electronice și/sau serviciului de comunicații electronice accesibil publicului, care se exemplifică prin acțiuni accidentale sau intenționate, cum ar fi, dar nu se limitează la:

- a) dezvăluirea neautorizată a informațiilor;
- b) distrugerea neautorizată sau modificarea datelor, echipamentelor sau altor resurse;
- c) furtul, îndepărtarea sau pierderea resurselor;
- d) întreruperea sau refuzul serviciilor;
- e) identificarea în mod fraudulos cu o entitate autorizată.

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

3) *incident cu impact semnificativ* – acel incident care afectează un număr mai mare de 1000 de conexiuni, într-un interval de timp de cel puțin 60 de minute, măsurat din momentul în care serviciul începe să se degradeze sau s-a întrerupt, până în momentul în care acesta este adus la parametrii normali de funcționare. O conexiune reprezintă:

- a) în cazul serviciilor de acces la Internet la puncte fixe: o conexiune de acces la Internet;
- b) în cazul serviciilor de transmisiuni de date la puncte fixe: o conexiune de acces la servicii de transmisiuni de date;

c) 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;

d) în cazul serviciilor de telefonie, acces la Internet și transmisiuni de date furnizate prin intermediul rețelelor publice mobile celulare terestre: o cartelă SIM activă;

e) în cazul serviciilor de retransmisie a serviciilor de programe audiovizuale: o conexiune de retransmisie a serviciilor de programe audiovizuale.

4) *măsuri de securitate* – mijloace (de natură administrativă, organizatorică, 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 publice de comunicații electronice și/sau a serviciilor de comunicații electronice accesibile publicului;

5) *resurse* – oricare din mijloacele care prezintă valori pentru furnizorul de rețele publice de comunicații electronice și/sau de servicii de comunicații electronice accesibile publicului, pentru operațiunile sale de afaceri și continuitatea acestora, și care includ:

a) informații: de rutare, de configurare a echipamentelor, referitoare la utilizatorii de servicii, referitoare la serviciile furnizate, la traficul efectuat, taxare, baze de date, documentație de sistem, manuale de utilizare, contracte și acorduri, proceduri operaționale, materiale pentru instruire, planuri pentru continuitatea afacerii, acorduri privind alternativele disponibile în cazuri de urgență, înregistrări etc.;

b) software: de control al comunicațiilor, de management al operațiunilor, de management al informațiilor privind utilizatorii, de taxare, de aplicații, de sistem, de dezvoltare și utilități etc.;

c) resurse fizice: clădiri, echipamente de comutare sau rutare, sisteme de transmisie, echipamente terminale, mediile utilizate pentru transmiterea semnalelor, servere și stații de lucru etc.;

d) servicii: de procesare a informațiilor, de rețea, utilități suport (alimentare cu energie electrică, iluminat, control al temperaturii și umidității, stingere a incendiilor) etc.;

e) resurse umane: ingineri de comunicații, specialiști IT etc.,

f) resurse intangibile: controlul organizației, „*know-how*” etc.;

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

## **II. MODALITATEA DE IMPLEMENTARE A MĂSURILOR MINIME DE SECURITATE**

**3.** Furnizorii de rețele publice de comunicații electronice și/sau de servicii de comunicații electronice accesibile publicului, în continuare denumiți furnizori, potrivit prevederilor art. 21 din Legea comunicațiilor electronice nr. 241/2007 au obligația:

1) de a lua toate măsurile tehnice și organizatorice adecvate pentru a administra riscurile care pot afecta securitatea rețelelor și serviciilor 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) de a lua toate măsurile tehnice și organizatorice adecvate pentru a administra riscurile care pot afecta rețelele și serviciile 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.

**4.** Măsurile minime de securitate pe care trebuie să le stabilească și să le implementeze furnizorii, astfel încât să îndeplinească obligațiile prevăzute la pct. 3 din prezentele Cerințe vor viza cel puțin următoarele domenii:

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

**5.** Cu referință la domeniul „*politica de securitate și managementul riscului*” specificat la pct. 4 subpct. 1), furnizorii au obligația:

- 1) să stabilească o politică de securitate și integritate a rețelelor 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, amenințările, 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.).

**6.** Cu referință la domeniul „*securitatea resurselor umane*” specificat la pct. 4 subpct.2), furnizorii au obligația:

- 1) să efectueze controale de verificare de fond a candidaților pentru angajare, a contractorilor și a terților în conformitate cu actele normative aplicabile, reglementările și etica stabilite pe intern, 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.

**7.** Cu referință la domeniul „*securitatea și integritatea rețelelor, infrastructurii asociate și informațiilor*” specificat la pct. 4 subpct.3), furnizorii au obligația:

1) să stabilească o securitate fizică adecvată a rețelei și infrastructurii asociate (stabilirea și menținerea unor măsuri care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundații, cutremure, explozii, tulburări publice și alte forme de dezastre naturale sau provocate de oameni);

2) să stabilească o securitate adecvată a utilităților-suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor;

3) să stabilească măsuri de securitate adecvate pentru accesul (logic) la rețea și la sistemele informatice;

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 cibernetice, inclusiv DoS (*Denial of Service* – refuzul/blocarea serviciului)/DDoS (*Distributed Denial of Service* – blocarea distribuită a serviciului).

**8.** Cu referință la domeniul „*managementul operațiunilor*” specificat la pct. 4 subpct. 4), 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.

**9.** Cu referință la domeniul „*managementul incidentelor*” specificat la pct. 4 subpct.5), furnizorii au obligația:

1) să stabilească procese și proceduri pentru managementul incidentelor care pot afecta 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 Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI) și către alte organe responsabile și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori de rețele și servicii de comunicații electronice afectați, media, clienți/utilizatori finali, parteneri de afaceri etc.).

**10.** Cu referință la domeniul „*managementul continuității afacerii*” specificat la pct.4 subpct. 6), 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 capacități de implementare a strategiei de continuitate și să stabilească planuri de continuitate și de recuperare.

**11.** Cu referință la domeniul „*monitorizare, testare și audit*” specificat la pct. 4 subpct. 7), 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 produselor program, 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.

12. Furnizorii au obligația de a evalua și, dacă este cazul, de a actualiza măsurile prevăzute la pct. 4 – 11 ori de câte ori este necesar, însă cel puțin o dată la 12 luni.

### **III. CIRCUMSTANȚELE, FORMATUL ȘI PROCEDURILE APLICATE RAPORTĂRII INCIDENTELOR CU IMPACT SEMNIFICATIV**

13. Furnizorii notifică ANRCETI și, după caz, alte organe împuternicite, în cel mai scurt timp, cu privire la orice incident cu impact semnificativ asupra furnizării rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului.

14. Furnizorii au obligația să desemneze o persoană/persoane responsabilă/responsabile de raportarea incidentelor cu impact semnificativ asupra securității și integrității rețelelor publice de comunicații electronice și serviciilor de comunicații electronice accesibile publicului și să transmită către ANRCETI datele de contact ale acesteia/acestora, în termen de cinci zile lucrătoare de la intrarea în vigoare a prezentelor Cerințe, precum și orice modificare a acestor date, în termen de cinci zile lucrătoare de la survenirea modificărilor.

15. În aplicarea pct. 13, furnizorul transmite 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 rețelei și serviciilor publice de comunicații electronice.

16. Notificarea inițială se transmite de către una dintre persoanele responsabile prevăzute la pct. 14, ca înscris în format electronic la adresa de poștă electronică a ANRCETI: [incidente@anrceti.md](mailto:incidente@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, de către alți furnizori, a rețelelor publice de comunicații electronice și serviciilor de comunicații electronice accesibile publicului pe piața națională de comunicații electronice;
- 4) estimarea efectelor în ceea ce privește apelarea numărului unic pentru apeluri de urgență 112;
- 5) descrierea sumară a cauzei/cauzelor care a/au provocat incidentul;
- 6) estimarea graficului de restabilire a furnizării rețelelor și serviciilor de comunicații electronice în parametrii normali de funcționare;
- 7) îndrumările oferite de furnizor clienților/utilizatorilor finali în vederea minimizării efectelor incidentului, dacă este cazul;
- 8) informațiile oferite publicului cu privire la existența incidentului, 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.

17. 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 [incidente@anrceti.md](mailto:incidente@anrceti.md).

**18.** În situația în care confirmarea primirii unui înscris în format electronic nu s-a realizat în condițiile pct. 17, 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.

**19.** În aplicarea pct. 13, furnizorii au obligația să transmită la ANRCETI o notificare finală privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor 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 la prezentele Cerințe.

**20.** În cazul în care, la momentul transmiterii notificării finale prevăzute la pct. 19 furnizorul nu are disponibile toate informațiile prevăzute în formularul-tip de raportare, acesta transmite 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.

**21.** Notificarea finală și notificarea suplimentară prevăzute la pct. 19 și respectiv pct. 20, se transmit la sediul ANRCETI, cu următoarele date de identificare: MD -2012, bd. Ștefan cel Mare, 134, mun. Chișinău, Republica Moldova; tel.:+373-22251317, fax: +373-22222885, 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 la adresa de poștă electronică [incidente@anrceti.md](mailto:incidente@anrceti.md), căruia i s-a aplicat o semnătură digitală autentică, bazată pe un certificat al cheii publice, nesuspendat sau nerevocat la momentul respectiv.

**22.** Este considerată dată 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.

**23.** Anual, către data de 31 ianuarie, furnizorii 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.

**24.** Formularul-tip de raportare prevăzut la pct. 19 poate fi obținut de la sediul ANRCETI, sau de pe pagina de Internet a ANRCETI.

#### **IV. CONDIȚIILE ȘI MODALITĂȚILE DE INFORMARE A PUBLICULUI CU PRIVIRE LA EXISTENȚA INCIDENTELOR CU IMPACT SEMNIFICATIV**

**25.** Ca urmare a primirii notificării inițiale prevăzute la pct. 15 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 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 asigură informarea publicului cu privire la existența situației prevăzute la pct. 24, 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. 25 modalitățile și condițiile de informare a publicului, furnizorul va realiza informarea publicului cel puțin prin una dintre modalitățile prevăzute la pct. 25.

## **V. MODALITĂȚILE DE VERIFICARE A RESPECTĂRII CERINȚELOR PRIVIND MĂSURILE MINIME DE SECURITATE ȘI EVALUAREA SECURITĂȚII ȘI INTEGRITĂȚII REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE**

**28.** Furnizorii asigură oferirea tuturor informațiilor și documentelor solicitate de ANRCETI în termenele și la nivelul de detaliere indicate de ANRCETI, necesare pentru:

1) evaluarea securității și integrității rețelelor publice de comunicații electronice și serviciilor de comunicații electronice accesibile publicului, inclusiv a politicilor interne de securitate aplicabile;

2) verificarea respectării de către furnizori a prezentelor Cerințe în partea ce ține de măsurile minime de securitate ce trebuie luate de către aceștia;

3) verificarea respectării de către furnizori a măsurilor stabilite de către aceștia pentru garantarea securității și integrității rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, în cazul apariției incidentelor cu impact semnificativ asupra securității și integrității rețelelor și/sau serviciilor;

4) verificarea și evaluarea managementului operațiunilor, incidentelor, continuității afacerii și procesului de monitorizare.

**29.** La solicitarea ANRCETI, care nu poate fi mai des de o dată pe an, furnizorii inițiază pe cont propriu un audit al securității realizat de un organ calificat, independent și transmit ANRCETI rezultatele auditului în termen de cinci zile lucrătoare din data finisării acestuia.

**30.** Dacă în rezultatul acțiunilor prevăzute la pct. 27 și 28, ANRCETI constată încălcarea de către furnizori a prevederilor prezentelor Cerințe, insuficiența măsurilor stabilite de furnizori pentru garantarea securității și integrității rețelelor și/sau serviciilor sau nerespectarea de către furnizori a măsurilor proprii de securitate, furnizorii vizați au obligația de a lua toate măsurile indicate de ANRCETI cu privire la, după caz, stabilirea politicilor, strategiilor, proceselor și procedurilor de asigurare a securității și integrității rețelelor și serviciilor, infrastructurii asociate, resurselor umane și informațiilor.



<b>FORMULAR DE RAPORTARE A INCIDENTELOR CARE AU AFECTAT SECURITATEA ȘI INTEGRITATEA REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE</b>	
<b>1. Furnizor:</b>	
<b>2. Data și ora</b>	
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: _____
<b>3. Impactul incidentului și tipul cauzei</b>	
<b>3.1 Serviciul/serviciile afectate:</b>	<b>Numărul de conexiuni afectate:</b>
<input type="checkbox"/> <b>Servicii de telefonie accesibile publicului:</b>	
<input type="checkbox"/> furnizate în baza tehnologiei TDM prin intermediul unor rețelelor publice terestre cu acces la puncte fixe sau cu mobilitate limitată	
<input type="checkbox"/> furnizate prin intermediul propriei rețele publice mobile celulare terestre	
<input type="checkbox"/> furnizate prin intermediul unor rețele publice mobile celulare terestre ale altor furnizori (de tip MVNO)	
<input type="checkbox"/> furnizate în baza protocolului IP (IP-telefonie, VoIP) prin intermediul accesului în bandă largă prestat de furnizorul serviciului de telefonie	
<input type="checkbox"/> furnizate în baza protocolului IP (IP-telefonie, VoIP) prin Internetul deschis (acces la Internet negestionat de furnizorul serviciului de telefonie)	
<input type="checkbox"/> furnizate prin intermediul propriilor telefoane publice cu plată sau cabine telefonice	
<input type="checkbox"/> furnizate prin intermediul unor rețele publice cu acces prin satelit	
<input type="checkbox"/> <b>Servicii de linii închiriate</b>	
<input type="checkbox"/> furnizate prin infrastructuri de fibră optică	
<input type="checkbox"/> furnizate prin infrastructuri de cupru	
<input type="checkbox"/> furnizate prin infrastructuri de radiorelee	
<input type="checkbox"/> <b>Servicii de transmisiuni de date (inclusiv SMS și VPN):</b>	
<input type="checkbox"/> furnizate la puncte fixe	
<input type="checkbox"/> furnizate la puncte cu mobilitate limitată	
<input type="checkbox"/> SMS (numai în cazul rețelelor mobile celulare terestre)	
<input type="checkbox"/> furnizate prin intermediul propriei rețele publice mobile celulare terestre	
<input type="checkbox"/> furnizate prin intermediul unor rețele publice mobile celulare terestre ale altor furnizori (de tip MVNO)	

<input type="checkbox"/> furnizate prin intermediul unor rețele publice cu acces prin satelit	
<b>Servicii de acces la Internet:</b>	
<input type="checkbox"/> furnizate prin tehnologia Dial-up (numai pentru bucla locală)	
<input type="checkbox"/> furnizate prin conexiuni permanente la puncte fixe sau cu mobilitate limitată	
<input type="checkbox"/> furnizate prin intermediul propriei rețele publice mobile celulare terestre	
<input type="checkbox"/> furnizate prin intermediul unor rețele publice mobile celulare terestre ale altor furnizori (de tip MVNO)	
<input type="checkbox"/> furnizate prin intermediul unor rețele publice cu acces prin satelit	
<input type="checkbox"/> <b>Servicii de retransmisie a serviciilor de programe audiovizuale:</b>	
<input type="checkbox"/> furnizate prin rețele publice terestre cu acces la puncte fixe sau cu mobilitate limitată (tip CATV, IPTV, DVB-C, MMDS, etc.)	
<input type="checkbox"/> furnizate prin rețele publice cu acces fix prin satelit (tip DTH)	
<input type="checkbox"/> furnizate prin rețele publice cu acces mobil prin satelit (tip S-DAB/DVB-S)	
<input type="checkbox"/> furnizate prin rețele de televiziune digitale terestre (tip DVB-T2)	
<input type="checkbox"/> furnizate prin intermediul rețelelor publice mobile celulare terestre (tip Mobile TV)	
<input type="checkbox"/> <b>Alte tipuri de servicii de comunicații electronice accesibile publicului decât cele de mai sus (de specificat: _____)</b>	
<b>3.2 Parametrii de impact:</b>	
Numărul total de conexiuni afectate de incident:	
Resursele/echipamentele afectate:	
Durata incidentului:	
Aria/răspândirea geografică:	
Impactul asupra apelurilor de urgență:	
<b>3.3 Descrierea incidentului:</b>	
<b>3.4 Cauza presupusă/stabilită a incidentului:</b>	
<input type="checkbox"/> Eroare umană	
<input type="checkbox"/> Eroare de sistem	
<input type="checkbox"/> Fenomen natural	
<input type="checkbox"/> Acțiune rău intenționată	
<input type="checkbox"/> Cauză externă/parte terță	

<b>3.5 Mai multe informații despre cauza incidentului:</b>
<b>4. Alte informații despre incident</b>
<b>4.1 Acțiuni de răspuns la incident (inclusiv momentul când au fost luate):</b>
<b>4.2 Măsurile luate sau preconizate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):</b>
<b>4.3 Alți furnizori de rețele și servicii de comunicații electronice afectați:</b>
<b>4.4 Alte observații:</b>

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

<b>1. Furnizor:</b>	
<i>Se completează cu denumirea furnizorului care trimite raportul către ANRCETI</i>	
<b>2. Data și ora</b>	
2.1 Data și ora la care s-a produs incidentul	<i>Se completează data și ora la care s-a produs incidentul, respectiv la care s-a descoperit incidentul. Formatul de introducere a datei este de tipul zz.ll.aaaa.</i>
2.2 Data și ora la care s-a descoperit incidentul	
<b>3. Impactul incidentului și tipul cauzei</b>	
<b>3.1 Serviciul/serviciile afectate și metoda de estimare:</b>	
<p>Se bifează serviciul/serviciile a cărui/căror furnizare a fost afectată de incident. Câmpul „Numărul de conexiuni afectate” din dreptul fiecărui tip de serviciu se completează corespunzător, fiecărui serviciu afectat în parte fiindu-i alocat numărul de conexiuni afectate de incident.</p> <p>O conexiune reprezintă:</p> <ul style="list-style-type: none"> <li>- în cazul serviciilor de acces la Internet la puncte fixe: o conexiune de acces la Internet;</li> <li>- în cazul serviciilor de transmisiuni de date la puncte fixe: o conexiune de acces la servicii de transmisiuni de date;</li> <li>- 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;</li> <li>- în cazul serviciilor de telefonie, acces la Internet și transmisiuni de date furnizate prin intermediul rețelelor publice mobile celulare terestre: o cartelă SIM activă;</li> <li>- în cazul serviciilor de retransmisie a serviciilor de programe audiovizuale liniare: o conexiune de retransmisie a serviciilor de programe audiovizuale.</li> </ul> <p>În cazul serviciilor furnizate prin intermediul unor rețele publice mobile celulare terestre, furnizorul va estima numărul de conexiuni afectate. Metoda de estimare a numărului de cartele SIM afectate de un incident este următoarea:</p> <p>În momentul apariției unui incident se identifică celulele afectate.</p> <p>Traficul total pierdut la nivelul tuturor celulelor afectate (<math>T_{pierdut}</math>) 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.</p> <p>Traficul total înregistrat la nivelul rețelei (<math>T_{rețea}</math>) se consideră a fi suma traficului din toate celulele din rețea în intervalul de timp respectiv, în săptămâna anterioară.</p> <p>Numărul de cartele SIM afectate se calculează astfel:</p> $N_{cartele\ SIM\ afectate} = N_{ds} \frac{T_{pierdut}}{T_{rețea}}$ <p><math>N_{ds}</math> 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.</p>	

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.	
<b>3.2 Parametrii de impact:</b>	
Numărul total de conexiuni afectate de incident:	<i>Se specifică numărul total de conexiuni afectate de incident. Acest număr se calculează ca sumă a numărului de conexiuni afectate pe fiecare tip de serviciu.</i>
Resursele/echipamentele afectate:	<p>Se specifică resursele/echipamentele afectate de incident. Ca exemplu, este prezentată în continuare o listă de resurse ce pot fi afectate:</p> <ul style="list-style-type: none"> <li>- stații de bază pentru PLMN (<i>BSC, BTS, RNC, NodeB etc.</i>);</li> <li>- rețea locală (cabluri de cupru, fibră etc.);</li> <li>- cabinete stradale;</li> <li>- echipamente de comutare sau rutare (comutatoare de rețea, routere, multiplexoare etc.);</li> <li>- noduri de transmisiuni;</li> <li>- centre de comutație;</li> <li>- centre de mesaje;</li> <li>- registre de utilizatori (<i>HLR, VLR, AuC, Home Subscriber Server etc.</i>);</li> <li>- <i>backbone</i>;</li> <li>- interconectări;</li> <li>- echipamente pentru alimentarea de rezervă cu energie electrică (baterii, generatoare);</li> <li>- sisteme de alimentare cu energie electrică;</li> <li>- alte resurse/echipamente (de specificat _____)</li> </ul>
Durata incidentului:	<i>Se specifică intervalul de timp dintre momentul în care serviciul începe să 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 specifică regiunea geografică afectată de incident (de exemplu: municipiul, orașul, raionul, satul).</i>
Impactul asupra apelurilor de urgență:	<i>Se specifică modul în care au fost afectate comunicațiile către numărul unic pentru apeluri de urgență 112 sau, după caz, către serviciilor de urgență la numerele 901, 902, 903, 904;</i>
<b>3.3 Descrierea incidentului:</b>	
Se completează cu orice informații și detalii disponibile privind apariția, dezvoltarea, impactul incidentului și modalitatea în care au fost afectate resursele/echipamentele.	
<b>3.4 Cauza presupusă/stabilită a incidentului:</b>	
<p>Se bifează cauza/cauzele incidentului: eroare umană, eroare de sistem, fenomen natural, acțiune rău intenționată și cauză externă/parte terță. Despre faptul că motivul incidentului este presupus sau stabilit se specifică prin informația de detaliere de la pct.3.5.</p> <p>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).</p> <p>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</p>	

a unui echipament de comunicații electronice). În acest caz, furnizorul va bifa cauza inițială.
<b>3.5 Mai multe informații despre cauza incidentului:</b>
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.
<b>4. Alte informații despre incident</b>
<b>4.1 Acțiuni de răspuns la incident (inclusiv momentul când au fost luate):</b>
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.
<b>4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):</b>
Câmpul va cuprinde descrierea detaliată a acțiunilor realizate pentru a minimiza nivelul de risc și pentru a preveni reapariția incidentului (de exemplu: revizuire măsuri de securitate și proceduri, renegociere SLA-uri, instruire de personal, achiziție de echipamente sau sisteme de <i>backup</i> etc), precum și momentul când au fost luate sau când vor fi luate aceste măsuri.
<b>4.3 Alți furnizori de rețele și servicii de comunicații electronice afectați:</b>
Acest câmp se completează cu detalii despre furnizorul și resursele/serviciile acestuia afectate de incident. De asemenea, se descrie modul de colaborare cu alți furnizori în vederea soluționării incidentului, inclusiv acțiunile comune de răspuns la incident.
<b>4.4 Alte observații:</b>
Acest câmp se completează cu orice alte detalii sau observații care nu au fost incluse în câmpurile de mai sus.