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

H O T Ă R Â R E
pentru aprobarea Modalităţii de implementare a măsurilor minime de securitate şi integritate a reţelelor publice de comunicaţii electronice şi/sau serviciilor de comunicaţii electronice accesibile publicului

nr. 60 din 24.12.2019

Monitorul Oficial nr.7-13/32 din 17.01.2020

* * *

ÎNREGISTRAT:
Ministerul Justiţiei
al Republicii Moldova
nr.1523 din 3 ianuarie 2020
Ministru _____ Fadei NAGACEVSCHI

În temeiul art.21 alin.(4) din Legea comunicaţiilor electronice nr.241/2007 (republicată în Monitorul Oficial al Republicii Moldova, 2017, nr.399-410, art.679), cu modificările ulterioare,

În vederea realizării acţiunii prevăzute la pct.2 subpct.2.2 din Planul de acţiuni privind implementarea Programului naţional 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 administraţie

HOTĂRĂŞTE:

1. Se aprobă Modalitatea de implementare a măsurilor minime de securitate şi integritate a reţelelor publice de comunicaţii electronice şi/sau serviciilor de comunicaţii electronice accesibile publicului (se anexează).

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

PREŞEDINTELE
CONSILIULUI DE ADMINISTRAŢIE AL ANRCETI Octavian RĂU

Membri **Andrei Muntean**
Marian Pocaznoi

Nr.60. Chişinău, 24 decembrie 2019.

Anexă
la Hotărârea Consiliului de
administraţie al ANRCETI
nr.60 din 24 decembrie 2019

Modalitatea de implementare
a măsurilor minime de securitate şi integritate a reţelelor publice de comunicaţii electronice şi/sau serviciilor de comunicaţii electronice accesibile publicului

Secţiunea 1
DISPOZIŢII GENERALE

1. Modalitatea de implementare a măsurilor minime de securitate şi integritate a reţelelor publice de comunicaţii electronice şi/sau serviciilor de comunicaţii electronice accesibile publicului (în continuare – prezenta Modalitate de implementare) stabileşte:

1) cerinţe privind implementarea măsurilor minime de securitate;

2) circumstanţele, formatul şi procedurile aplicate raportării incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor publice de comunicaţii electronice şi serviciilor de comunicaţii electronice accesibile publicului;

3) condiţiile şi modalităţile de informare a publicului cu privire la existenţa incidentelor menţionate la subpunctul 2);

4) modalităţile de verificare a respectării cerinţelor privind măsurile minime de securitate şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

2. În înţelesul prezentei Modalităţi de implementare, următorii termeni se definesc astfel:

1) ameninţare – circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii reţelei publice de comunicaţii electronice şi/sau serviciului de comunicaţii electronice accesibil publicului, care se exemplifică prin acţiuni accidentale sau intenţionate, cum ar fi, dar nu se limitează la:

a) dezvăluirea neautorizată a informaţiilor;

b) distrugerea sau modificarea neautorizată a 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 ameninţa, direct sau indirect, securitatea şi integritatea reţelelor publice de comunicaţii electronice şi serviciilor de comunicaţii electronice accesibile publicului (efectele cauzate de lucrările de întreţinere a reţelei, programate şi anunţate din timp utilizatorilor, nu sunt considerate incidente);

3) incident cu impact semnificativ – acel incident care afectează un număr mai mare de 2000 de conexiuni, într-un interval de timp de cel puţin 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 funcţionare. 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 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;

d) în cazul serviciilor de telefonie, acces la Internet şi transmisiuni de date furnizate prin intermediul reţelelor 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, acţiuni, planuri, echipamente, facilităţi, proceduri, tehnici etc. menite să elimine ori să reducă riscurile privind securitatea şi integritatea reţelelor publice de comunicaţii electronice şi/sau a serviciilor de comunicaţii electronice accesibile publicului;

5) resurse – oricare din mijloacele care prezintă valori pentru furnizorul de reţele publice de comunicaţii electronice şi/sau de servicii de comunicaţii electronice accesibile publicului, pentru operaţiunile sale de afaceri şi continuitatea acestora, şi care includ:

a) informaţii: de rutare, de configurare a echipamentelor, referitoare la utilizatorii de servicii, referitoare la serviciile furnizate, la traficul efectuat, taxare, baze de date, documentaţie de sistem, manuale de utilizare, contracte şi acorduri, proceduri operaţionale, materiale pentru instruire, planuri pentru continuitatea afacerii, acorduri privind alternativele disponibile în cazuri de urgenţă, dovezi de audit, înregistrări etc.;

b) software*:* de control al comunicaţiilor, de management al operaţiunilor, de management al informaţiilor privind utilizatorii, de taxare, de aplicaţii, de sistem, de dezvoltare şi utilităţi etc.;

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

d) servicii: de procesare a informaţiilor, de reţea, utilităţi suport (alimentare cu energie electrică, iluminat, control al temperaturii şi umidităţii, stingere a incendiilor) etc.;

e) resurse umane: ingineri de comunicaţii, specialişti IT etc.;

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

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

Secţiunea a 2-a
CERINŢE PRIVIND IMPLEMENTAREA MĂSURILOR MINIME DE SECURITATE

3. Furnizorii de reţele publice de comunicaţii electronice şi/sau de servicii de comunicaţii electronice accesibile publicului, în continuare denumiţi furnizori, potrivit prevederilor art.21 din Legea comunicaţiilor electronice nr.241/2007 au obligaţia:

1) de a lua toate măsurile tehnice şi organizatorice adecvate pentru a administra riscurile care pot afecta securitatea reţelelor şi serviciilor de comunicaţii electronice astfel, încât să asigure un nivel de securitate adecvat şi 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 costurile implementării în raport cu riscurile şi cu natura datelor cu caracter personal a căror protecţie trebuie asigurată;

2) de a lua toate măsurile tehnice şi organizatorice adecvate pentru a administra riscurile care pot afecta reţelele şi serviciile de comunicaţii electronice, în scopul garantării integrităţii reţelelor şi al asigurării continuităţii furnizării serviciilor prin intermediul acestor reţele;

3) de a colabora, după caz, cu alţi furnizori pentru implementarea măsurilor prevăzute la subpct.1) şi 2).

4. Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru securitate, furnizorul implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând măsurile minime de securitate pe care trebuie să le stabilească şi să le implementeze furnizorii, astfel încât să îndeplinească obligaţiile prevăzute la pct.3 din prezenta Modalitate de implementare vor viza cel puţin următoarele domenii:

1) politica de securitate şi managementul riscului;

2) securitatea resurselor umane;

3) securitatea şi integritatea reţelelor, infrastructurii asociate şi informaţiilor;

4) managementul operaţiunilor;

5) managementul incidentelor;

6) managementul continuităţii afacerii;

7) monitorizare, testare şi audit.

5. Cu referinţă la domeniul *„politica de securitate şi managementul riscului”* specificat la pct.4 subpct.1), furnizorii au obligaţia:

1) să aprobe o politică de securitate şi integritate a reţelelor 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).

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

1) să efectueze controale de verificare de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor în conformitate cu actele normative aplicabile, reglementările şi etica stabilite pe intern, 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.

7. Cu referinţă la domeniul *„securitatea şi integritatea reţelelor, infrastructurii asociate şi informaţiilor”* specificat la pct.4 subpct.3), furnizorii au obligaţia:

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

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

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

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

8. Cu referinţă la domeniul *„managementul operaţiunilor”* specificat la pct.4 subpct.4), 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.

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

1) să stabilească procese şi proceduri pentru managementul incidentelor care pot afecta 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 Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei (ANRCETI) şi către alte organe responsabile şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori de reţele şi servicii de comunicaţii electronice afectaţi, media, clienţi/utilizatori finali, parteneri de afaceri).

10. Cu referinţă la domeniul *„managementul continuităţii afacerii”* specificat la pct.4 subpct.6), furnizorii au obligaţia:

1) să stabilească o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor 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.

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

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.

12. Furnizorii au obligaţia de a evalua şi, dacă este cazul, de a actualiza măsurile prevăzute la pct.4 – 11 ori de câte ori este necesar, însă cel puţin o dată la doi ani. Pentru implementarea unor măsuri eficiente în domeniul managementului incidentelor pot fi utilizate standarde moldoveneşti şi recomandări tehnice internaţionale precum:

1) SM ISO/IEC 27035-2:2017, Tehnologia informaţiei. Tehnici de securitate. Managementul incidentelor de securitate a informaţiei. Partea 2: Linii directoare pentru planificarea şi pregătirea reacţionării la incidente;

2) SM EN ISO/IEC 27001:2017, Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe;

3) SM EN ISO/IEC 27002:2017, Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei;

4) SM ISO/IEC 27011:2017, Tehnologia informaţiei. Tehnici de securitate. Cod de bune practici pentru managementul securităţii informaţiei bazate pe ISO/IEC 27002 pentru organizaţiile din telecomunicaţii;

5) SM EN ISO 22301:2A16, Securitate societală. Sisteme de management al continuităţii activităţii. Cerinţe;

6) recomandarea ITU-T X.1056 – Ghid de gestionare a incidentelor de securitate pentru organizaţiile de telecomunicaţii.

Secţiunea a 3-a
CIRCUMSTANŢELE, FORMATUL ŞI PROCEDURILE APLICATE RAPORTĂRII INCIDENTELOR CU IMPACT SEMNIFICATIV

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

14. Furnizorii au obligaţia să desemneze o persoană/persoane responsabilă/responsabile de raportarea incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor publice de comunicaţii electronice şi serviciilor de comunicaţii electronice accesibile publicului şi să transmită către ANRCETI datele de contact ale acesteia/acestora, în termen de cinci zile lucrătoare de la intrarea în vigoare a prezentei Modalităţi de implementare, precum şi 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, 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 reţelei şi serviciilor publice de comunicaţii electronice, conform formularului-tip de raportare prevăzut de Anexa 1. În cazul în care nu sunt disponibile toate informaţiile prevăzute de Anexa 1 şi relevante cazului, fiind necesară investigarea mai amănunţită a incidentului, furnizorului i se permite să efectueze notificarea respectivă reieşind din datele disponibile şi cunoscute la ora raportării, cu menţiunea „notificare iniţială”, sau să efectueze o notificare iniţială în forma aleasă de el, ţinând cont de cerinţele şi informaţiile prevăzute în pct.16.

16. Notificarea iniţială în forma aleasă de furnizor, menţionată la pct.15, se transmite cu denumirea subiectului „Notificare iniţială privind incident cu impact semnificativ” de către una dintre persoanele responsabile prevăzute la pct.14, ca înscris în format electronic la adresa de poştă electronică a ANRCETI: office@anrceti.md, şi va cuprinde cel puţin următoarele elemente:

1) denumirea furnizorului;

2) se specifică dacă este vorba despre o primă sau o a doua informare;

3) ora identificării/constatării;

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

5) estimarea ariei geografice afectate, a numărului de conexiuni afectate, precum şi a efectelor incidentului asupra furnizării, de către alţi furnizori, a reţelelor publice de comunicaţii electronice şi serviciilor de comunicaţii electronice accesibile publicului pe piaţa naţională de comunicaţii electronice;

6) estimarea efectelor în ceea ce priveşte apelarea numărului unic pentru apeluri de urgenţă 112;

7) descrierea sumară a cauzei/cauzelor care a/au provocat incidentul, dacă a fost posibilă stabilirea acestei în timpul scurs de la identificarea/constatarea incidentului;

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

9) îndrumările oferite de furnizor clienţilor/utilizatorilor finali în vederea minimizării efectelor incidentului, dacă este cazul;

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

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

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

17. Este considerată dată a transmiterii notificării iniţiale menţionate la pct.15 ziua în care aceasta a fost expediată respectând cerinţa privind denumirea subiectului şi în timpul orelor de program al ANRCETI, sau următoarea zi lucrătoare.

18. ANRCETI, în ziua transmiterii înscrisului în format electronic, răspunde la adresa de e-mail a persoanei responsabile a furnizorului care a trimis Notificarea iniţială cu privire la recepţionarea mesajului.

19. În cazul în care a efectuat o notificare iniţială conform pct.15, furnizorul are obligaţia să transmită la ANRCETI o notificare finală privind existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor 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 la prezenta Modalitate de implementare.

20. În cazul în care, la momentul transmiterii notificării finale prevăzute la pct.19 furnizorul nu are disponibile toate informaţiile prevăzute în formularul-tip de raportare, acesta transmite o notificare suplimentară cu informaţiile respective, completând formularul-tip de raportare prevăzut în Anexa 1, imediat ce acestea sunt disponibile, dar nu mai târziu de 3 săptămâni de la detectarea incidentului cu impact semnificativ.

21. Notificarea finală şi notificarea suplimentară prevăzute la pct.19 şi respectiv pct.20, se transmit la sediul ANRCETI, cu următoarele date de identificare: MD-2012, bd.Ştefan cel Mare, 134, mun.Chişinău, 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 poştal;

3) printr-un înscris în format electronic la adresa de poştă electronică office@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 corespondenţei de intrare al ANRCETI, 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.

23. Formularul-tip de raportare prevăzut la pct.19 poate fi obţinut de la sediul ANRCETI, sau de pe pagina oficială a ANRCETI.

Secţiunea a 4-a
CONDIŢIILE ŞI MODALITĂŢILE DE INFORMARE A PUBLICULUI CU PRIVIRE LA EXISTENŢA INCIDENTELOR CU IMPACT SEMNIFICATIV

24. Ca urmare a primirii notificării prevăzute la pct.15, 19 sau 20 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 de comunicaţii electronice, prin intermediul paginii de Internet a ANRCETI, sau poate solicita furnizorului să informeze publicul în acest sens.

25. La solicitarea ANRCETI, furnizorul asigură informarea publicului cu privire la existenţa situaţiei prevăzute la pct.24, 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.

26. În cazul în care ANRCETI nu a stabilit prin solicitarea prevăzută la pct.25 modalităţile şi condiţiile de informare a publicului, furnizorul va realiza informarea publicului cel puţin prin una dintre modalităţile prevăzute la pct.25.

Secţiunea a 5-a
MODALITĂŢILE DE VERIFICARE A RESPECTĂRII CERINŢELOR PRIVIND MĂSURILE MINIME DE SECURITATE ŞI EVALUAREA SECURITĂŢII ŞI INTEGRITĂŢII REŢELELOR ŞI SERVICIILOR DE COMUNICAŢII ELECTRONICE

27. Furnizorii asigură oferirea tuturor informaţiilor şi documentelor solicitate de ANRCETI în termenele şi la nivelul de detaliere indicate de ANRCETI, necesare pentru:

1) evaluarea securităţii şi integrităţii reţelelor publice de comunicaţii electronice şi serviciilor de comunicaţii electronice accesibile publicului, inclusiv a politicilor interne de securitate aplicabile;

2) verificarea respectării de către furnizori a prezentei Modalităţi de implementare în partea ce ţine de măsurile minime de securitate ce trebuie luate de către aceştia;

3) verificarea respectării de către furnizori a măsurilor stabilite de către aceştia pentru garantarea securităţii şi integrităţii reţelelor publice de comunicaţii electronice şi/sau serviciilor de comunicaţii electronice accesibile publicului, în cazul apariţiei incidentelor cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi/sau serviciilor;

4) verificarea şi evaluarea managementului operaţiunilor, incidentelor, continuităţii afacerii şi procesului de monitorizare.

28. La solicitarea ANRCETI, care nu poate fi mai des de o dată pe an, furnizorii iniţiază pe cont propriu un audit al securităţii realizat de un organism calificat, independent şi transmit ANRCETI rezultatele auditului în termen de cinci zile lucrătoare din data finisării acestuia.

29. Dacă în rezultatul acţiunilor prevăzute la pct.27 şi 28, ANRCETI constată încălcarea de către furnizori a prevederilor prezentei Modalităţi de implementare, insuficienţa măsurilor stabilite de furnizori pentru garantarea securităţii şi integrităţii reţelelor şi/sau serviciilor sau nerespectarea de către furnizori a măsurilor proprii de securitate, furnizorii vizaţi au obligaţia de a lua toate măsurile indicate de ANRCETI cu privire la, după caz, stabilirea politicilor, strategiilor, proceselor şi procedurilor de asigurare a securităţii şi integrităţii reţelelor şi serviciilor, infrastructurii asociate, resurselor umane şi informaţiilor.

Anexa nr.1
la Modalitatea de implementare a măsurilor
minime de securitate şi integritate a reţelelor
publice de comunicaţii electronice şi/sau serviciilor
de comunicaţii electronice accesibile publicului

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 *(dacă se cunosc; dacă este necesar, se poate face o estimare)*	Data: Ora:
2.2 Data şi ora la care a fost identificat/constatat incidentul	Data: Ora:
3. Impactul incidentului şi tipul cauzei	
3.1 Serviciul/serviciile afectate:	**Numărul de conexiuni afectate:**
□ **Servicii de telefonie accesibile publicului:**	
□ *furnizate în baza tehnologiei TDM prin intermediul unor reţele publice terestre cu acces la puncte fixe sau cu mobilitate limitată*	
□ *furnizate prin intermediul propriei reţele publice mobile celulare terestre*	
□ *furnizate prin intermediul unor reţele publice mobile celulare terestre ale altor furnizori (de tip MVNO)*	
□ *furnizate în baza protocolului IP (IP-telefonie, VoIP) prin intermediul accesului în bandă largă prestat de furnizorul serviciului de telefonie*	
□ *furnizate în baza protocolului IP (IP-telefonie, VoIP) prin Internetul deschis (acces la Internet negestionat de furnizorul serviciului de telefonie)*	
□ *furnizate prin intermediul propriilor telefoane publice cu plată sau cabine telefonice*	
□ *furnizate prin intermediul unor reţele publice cu acces prin satelit*	
□ *furnizare servicii SMS aferente serviciilor de telefonie mobilă accesibile publicului*	
□ **Servicii de linii închiriate**	
□ *furnizate prin infrastructuri de fibră optică*	
□ *furnizate prin infrastructuri de cupru*	
□ *furnizate prin infrastructuri de radiorelee*	
□ **Servicii de transmisiuni de date (inclusiv VPN):**	
□ *furnizate la puncte fixe*	
□ *furnizate la puncte cu mobilitate limitată*	
□ *furnizate prin intermediul propriei reţele publice mobile celulare*	

terestre	
□ *furnizate prin intermediul unor reţele publice mobile celulare terestre ale altor furnizori (de tip MVNO)*	
□ *furnizate prin intermediul unor reţele publice cu acces prin satelit*	
Servicii de acces la Internet:	
□ *furnizate prin conexiuni permanente la puncte fixe sau cu mobilitate limitată*	
□ *furnizate prin intermediul propriei reţele publice mobile celulare terestre*	
□*furnizate prin intermediul unor reţele publice mobile celulare terestre ale altor furnizori (de tip MVNO)*	
□ *furnizate prin intermediul unor reţele publice cu acces prin satelit*	
□ ***Servicii de retransmisie a serviciilor de programe audiovizuale:***	
□ *furnizate prin reţele publice terestre cu acces la puncte fixe sau cu mobilitate limitată(tip CATV, IPTV, DVB-C, MMDS, etc.)*	
□ *furnizate prin reţele publice cu acces fix prin satelit (tip DTH)*	
□ *furnizate prin reţele publice cu acces mobil prin satelit (tip S-DAB/DVB-S)*	
□ *furnizate prin reţele de televiziune digitale terestre (tip DVB-T2)*	
□ *furnizate prin intermediul reţelelor publice mobile celulare terestre (tip Mobile TV)*	
□ ***Alte tipuri de servicii de comunicaţii electronice accesibile publicului decât cele de mai sus*** *(de specificat: _____)*	
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 Cauza presupusă/stabilită a incidentului:	
□ Eroare umană	
□ Eroare de sistem	
□ Fenomen natural	
□ Acţiune rău intenţionată	
□ Cauză externă/parte terţă	
□ Altă cauză (*a se indica*)	
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 preconizate 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 nr.2
la Modalitatea de implementare a măsurilor
minime de securitate şi integritate a reţelelor
publice de comunicaţii electronice şi/sau serviciilor
de comunicaţii electronice accesibile publicului

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

1. Furnizor:	
Se completează cu denumirea furnizorului care trimite raportul către ANRCETI	
2. Data şi ora	
2.1 Data şi ora la care s-a produs Incidentul *(dacă se cunosc; dacă este necesar, se poate face o estimare)*	*Se completează data şi ora la care s-a produs incidentul, respectiv la care s-a identificat/constatat incidentul. Formatul de introducere a datei este de tipul zz.ll.aaaa.*
2.2 Data şi ora la care s-a identificat/constatat incidentul	
3. Impactul incidentului şi tipul cauzei	
3.1 Serviciul/serviciile afectate şi metoda de estimare:	
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. 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 publice mobile celulare terestre: o cartelă SIM activă; - în cazul serviciilor de retransmisie a serviciilor de programe audiovizuale liniare: o conexiune de retransmisie a serviciilor de programe audiovizuale. În cazul serviciilor furnizate prin intermediul unor reţele 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: 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 specifică numărul total de conexiuni afectate de incident. Acest număr se calculează ca sumă a numărului de conexiuni afectate pe fiecare tip de serviciu.*
Resursele/echipamentele afectate:	Se specifică 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; - alte resurse/echipamente (de specificat _____)
Durata incidentului:	*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 iniţiali. Timpul va fi exprimat în minute.*
Aria/răspândirea geografică:	*Se specifică regiunea geografică afectată de incident (de exemplu: municipiul, oraşul, raionul, satul).*
Impactul asupra apelurilor de urgenţă:	*Se specifică modul în care au fost afectate comunicaţiile către numărului unic pentru apeluri de urgenţă 112 sau, după caz, către serviciilor de urgenţă la numerele 901, 902, 903, 904;*

3.3 Descrierea incidentului:

Se completează cu orice informaţii şi detalii disponibile privind apariţia, dezvoltarea, impactul incidentului şi modalitatea în care au fost afectate resursele/echipamentele.

3.4 Cauza presupusă/stabilită a incidentului:

Se bifează cauza/cauzele incidentului: eroare umană, eroare de sistem, fenomen natural, acţiune rău intenţionată şi cauză externă/parte terţă. Despre faptul că motivul incidentului este presupus sau stabilit se specifică prin informaţia de detaliere de la pct.3.5.

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 incident. 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.