

În temeiul prevederilor art. 3 lit. d), art. 10 alin. (1) pct. 1 și art. 12 alin. (3) din Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010, cu modificările și completările ulterioare, precum și ale art. 46, 47 alin. (1), (2) și (4), art. 49 alin. (1) lit. a) și art. 49¹ alin. (1) din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare,

AUTORITATEA NAȚIONALĂ PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII

emite prezenta:

DECIZIE

privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului

Art. 1. – Prezenta decizie are ca obiect stabilirea:

a) măsurilor tehnice și organizatorice care trebuie luate de furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice;

b) circumstanțelor, formatului și procedurilor aplicabile notificării Autorității Naționale pentru Administrare și Reglementare în Comunicații, denumită în continuare *ANCOM*, de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, a unui incident de securitate care are un impact semnificativ asupra rețelelor sau serviciilor de comunicații electronice.

Art. 2. – (1) În înțelesul prezentei decizii, următorii termeni se definesc astfel:

1. *disponibilitate* - proprietatea de a fi accesibil și utilizabil la cerere de către o entitate autorizată;

2. *autenticitate* - proprietatea potrivit căreia o entitate este ceea ce pretinde a fi;

3. *integritate* - proprietatea de a fi exact și complet;

4. *confidențialitate* - proprietatea ca informația să nu fie disponibilă sau divulgată persoanelor, entităților sau proceselor neautorizate;

5. *incident de securitate care are un impact semnificativ* – acel incident care atinge cel puțin unul dintre următoarele praguri cantitative sau calitative:

a) praguri cantitative:

(i) disponibilitate – afectarea, din perspectiva disponibilității rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de rețelele ori serviciile de comunicații electronice respective sau accesibile prin intermediul acestora, în cazul a 5.000 de utilizatori, timp de cel puțin 60 de minute, sau în cazul în care se depășește pragul de 500.000 de „ore-utilizator”;

(ii) autenticitate, integritate sau confidențialitate - sunt afectați cel puțin 5.000 de utilizatori, indiferent de durata incidentului;

b) praguri calitative:

(i) incidente care afectează, direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112;

(ii) incidente cu impact transfrontalier;

(iii) incidente care afectează securitatea rețelelor și serviciilor altui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și îi cauzează acestuia un incident care are un impact semnificativ, în măsura în care această situație era cunoscută;

6. *măsurile de securitate* - mijloace adecvate, obiective și proporționale (de natură administrativă, managerială, tehnică sau juridică) de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, procese, practici, tehnici etc., menite să gestioneze în mod corespunzător, să elimine ori să reducă riscurile privind securitatea rețelelor sau a serviciilor de comunicații electronice;

7. *backup electric fix* - o soluție sau o combinație de soluții tehnice de alimentare cu energie electrică, staționare, instalate într-o locație care găzduiește echipamente de rețea de comunicații electronice, având rolul de asigurare a continuității în funcționare a echipamentelor de rețea, respectiv a serviciilor oferite utilizatorilor prin intermediul echipamentelor respective, în caz de întrerupere a alimentării cu energie electrică din rețeaua de distribuție;

8. *hub de transmisiuni* – un element de rețea care concentrează traficul generat de cel puțin alte 8 elemente de rețea (de exemplu, site-uri radio);

9. *ore-utilizator* - se determină utilizând următoarea formulă:

$$\frac{\text{număr utilizatori afectați de incident} \times \text{durata incidentului, exprimată în minute}}{60}$$

(2) În cuprinsul prezentei decizii sunt, de asemenea, aplicabile definițiile relevante prevăzute la art. 4 alin. (1) din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare, precum și la art. 3 alin. (1) din Ordonanța de urgență a Guvernului nr. 34/2008 privind organizarea și funcționarea Sistemului național unic pentru apeluri de urgență, aprobată cu modificări și completări prin Legea nr. 160/2008, cu modificările și completările ulterioare.

Art. 3. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua toate măsurile de securitate tehnice, inclusiv criptarea, după caz, și organizatorice adecvate, obiective și proporționale pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice, astfel încât să asigure un nivel de securitate corespunzător riscului identificat, ținând seama de stadiul actual al tehnologiei, și să prevină sau să minimizeze impactul incidentelor de securitate

asupra utilizatorilor și asupra altor rețele și servicii, precum și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.

(2) Măsurile de securitate pe care trebuie să le stabilească și să le implementeze furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, astfel încât să îndeplinească obligația prevăzută la alin. (1), vor viza cel puțin domeniile și obiectivele identificate în anexa nr. 1.

(3) Atunci când este justificat pe baza evaluării efective a riscurilor, măsurile luate de furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere, precum și de furnizorii de servicii de comunicații interpersonale bazate pe numere care nu exercită un control efectiv asupra transmiterii semnalului, pot exclude anumite obiective de securitate aferente domeniilor identificate în anexa nr. 1.

(4) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului care au un număr de cel puțin 100.000 de conexiuni vor transmite anual către ANCOM, până la data de 10 februarie a fiecărui an, măsurile de securitate existente la data de 31 decembrie a anului anterior raportării, pe structura domeniilor și obiectivelor de securitate identificate în anexa nr. 1, evidențiind totodată evoluțiile față de raportarea anterioară.

(5) Prima raportare în conformitate cu alin. (4) se va realiza până la data de 10 februarie 2025 și nu va conține informațiile referitoare la evoluția în timp a măsurilor de securitate.

(6) Prevederile alin. (4) nu se aplică furnizorilor de servicii de comunicații interpersonale care nu se bazează pe numere și furnizorilor de servicii de comunicații interpersonale bazate pe numere care nu exercită un control efectiv asupra transmiterii semnalului.

(7) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a evalua și, dacă este cazul, de a actualiza măsurile prevăzute la alin. (2) ori de câte ori este necesar, însă cel puțin o dată la 12 luni.

(8) Atunci când consideră necesar, ANCOM solicită furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului transmiterea, într-un termen stabilit de aceasta, dar care nu poate depăși 30 de zile de la primirea solicitării, a tuturor informațiilor necesare evaluării securității rețelelor și serviciilor, inclusiv a documentației ce a stat la baza implementării măsurilor de securitate, precum și a deciziei de excludere a anumitor obiective de securitate, în cazul furnizorilor prevăzuți la alin. (3).

Art. 4. – (1) În vederea creșterii nivelului de securitate a rețelelor și serviciilor de comunicații electronice, furnizorii de rețele publice de comunicații electronice care au un număr de cel puțin 100.000 de conexiuni sau care au rețele amplasate pe teritoriul a cel puțin 100 de unități administrativ-teritoriale de bază, din cel puțin 20 de județe, au obligația de a respecta următoarele valori minime ale duratelor de backup electric fix:

a) o oră – timp de backup electric fix standard, durată aplicabilă oricărui element de rețea situat în localitățile urbane;

b) 3 ore – timp de backup electric fix standard, durată aplicabilă oricărui element de rețea situat în afara localităților urbane;

c) 6 ore – timp de backup electric fix extins, durată aplicabilă următoarelor elemente de rețea: unități centrale de comutație/control, huburi de transmisiuni, elemente de rețea din locații cu acces fizic dificil și locații identificate statistic ca având incidență sau frecvență de apariție a avariilor electrice ridicate.

(2) Capacitatea de backup electric necesară în vederea respectării valorilor de la alin. (1) se va calcula avându-se în vedere puterea maximă absorbită de echipamentul de securizat, așa cum este aceasta marcată pe echipament sau declarată de producătorul acestuia.

(3) În calculul capacității de backup electric necesare în vederea respectării valorilor de la alin. (1) se va avea în vedere și puterea maximă absorbită de sistemele de climatizare, sistemele de supraveghere alarme externe și sistemele de control-acces.

(4) Prin excepție de la prevederile alin. (3), în calculul capacității de backup electric necesare în vederea respectării valorilor de la alin. (1) lit. a) și b) nu se va avea în vedere puterea maximă absorbită de sistemele de climatizare.

(5) Sunt exceptate de la prevederile alin. (1) lit. a) și b) echipamentele de acces radio din categoriile repetoarelor instalate în interiorul clădirilor, microcelulelor, precum și echipamentele de rețea fixă instalate în locațiile utilizatorilor finali sau în proximitatea locațiilor utilizatorilor finali.

(6) Dispozițiile alin. (5) nu se aplică echipamentelor care oferă servicii specifice tehnologiei mobile aferente rețelelor definite potrivit dispozițiilor art. 2 lit. f) din Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G, respectiv URLLC și mMTC.

(7) Furnizorii de rețele publice de comunicații electronice prevăzuți la alin. (1) vor transmite în format electronic către ANCOM, până la data de 10 februarie a fiecărui an, lista privind locațiile încadrabile la data de 31 decembrie a anului anterior în categoria specificată la alin. (1) lit. c).

(8) Prima raportare în conformitate cu alin. (7) se va realiza până la data de 10 februarie 2025.

Art. 5. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM o notificare privind existența unui incident de securitate care are un impact semnificativ.

(2) În aplicarea alin. (1), furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM o notificare inițială, până cel târziu la ora 13.00 a zilei lucrătoare următoare celei în care a fost detectat incidentul de securitate care are un impact semnificativ, cu excepția incidentelor care afectează mai mult de 100.000 utilizatori, care vor fi notificate până cel târziu la ora 13.00 a zilei calendaristice următoare celei în care a fost detectat incidentul.

(3) Notificarea inițială prevăzută la alin. (2) se transmite ca înscris în formă electronică la adresa de poștă electronică incidente@ancom.ro și va cuprinde cel puțin următoarele elemente:

a) data și ora detectării incidentului;

b) serviciile și/sau rețelele de comunicații electronice care sunt afectate de incident;

c) estimarea ariei geografice afectate, a numărului de utilizatori afectați, precum și a efectelor incidentului asupra rețelelor și serviciilor altor furnizori, pe piața națională de comunicații electronice sau pe cea din alt stat membru al Uniunii Europene;

d) estimarea efectelor în ceea ce privește rutarea comunicațiilor de urgență către Serviciul de urgență 112;

e) o descriere sumară a cauzei/cauzelor care a/au provocat incidentul;

f) estimarea graficului și a măsurilor de restabilire a furnizării rețelelor și serviciilor de comunicații electronice în parametri normali de funcționare;

g) informațiile oferite de furnizor utilizatorilor, inclusiv îndrumări în vederea minimizării efectelor incidentului, dacă este cazul.

(4) Notificarea inițială prevăzută la alin. (2) se transmite de către una dintre persoanele responsabile prevăzute la art. 7, iar, în cazul furnizorilor care au sub 5.000 de utilizatori, aceasta se va realiza de către reprezentantul legal sau de către un împuternicit al acestuia, care transmite în același timp și dovada calității de împuternicit al furnizorului.

(5) Este considerată dată a transmiterii înscrisului în formă electronică data confirmării primirii de către ANCOM a acestui înscris. ANCOM asigură fără întârziere și în mod automat confirmarea primirii înscrisului în formă electronică transmis la adresa de poștă electronică prevăzută la alin. (3).

(6) În situația în care confirmarea primirii unui înscris în formă electronică nu s-a realizat în condițiile alin. (5), este considerată dată a transmiterii data la care înscrisul în formă electronică a fost primit, astfel cum este aceasta atestată de calculatorul de primire al ANCOM.

(7) În aplicarea alin. (1), furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM o notificare finală privind existența unui incident de securitate care are un impact semnificativ, în termen de două săptămâni de la detectarea acestuia, completând informațiile aferente prin aplicația informatică prevăzută de dispozițiile art. 5 alin. (1) din Decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații nr. 336/2013 privind mijloacele și modalitatea de transmitere de către furnizori a unor documente, date sau informații către Autoritatea Națională pentru Administrare și Reglementare în Comunicații, cu modificările și completările ulterioare, prevederile acesteia fiind aplicabile în mod corespunzător.

(8) În cazul în care, la momentul transmiterii notificării finale prevăzute la alin. (7), furnizorii nu au disponibile toate informațiile prevăzute de câmpurile din aplicația informatică, aceștia au obligația de a transmite o notificare suplimentară cu informațiile respective, completând câmpurile lipsă, imediat ce informațiile sunt disponibile, dar nu mai târziu de 4 săptămâni de la detectarea incidentului de securitate care are un impact semnificativ. Dispozițiile alin. (7) se aplică în mod corespunzător.

(9) În situația în care un incident a fost finalizat și se cunosc toate informațiile cu privire la incident până la ora transmiterii notificării inițiale, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pot raporta incidentul direct în aplicația informatică prevăzută la alin. (7), completând informațiile aferente unei notificări finale.

(10) Câmpurile din aplicația informatică prevăzută la alin. (7) au la bază formularul-tip de raportare prevăzut în anexa nr. 2, iar completarea se face cu respectarea instrucțiunilor specificate în anexa nr. 3.

(11) Notificarea finală, precum și notificarea suplimentară prevăzute la alin. (7), respectiv alin. (8) se transmit ANCOM ca înscris în formă electronică căruia i s-a încorporat, atașat ori asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la data transmiterii și generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

Art. 6. – (1) Ca urmare a primirii notificării inițiale prevăzute la art. 5 alin. (2) și atunci când consideră că este în interesul public, ANCOM poate informa publicul cu privire la existența unui incident de securitate care are un impact semnificativ, prin intermediul paginii de internet a ANCOM și/sau prin orice alte mijloace, sau poate solicita furnizorului să informeze publicul în acest sens.

(2) La solicitarea ANCOM, furnizorul de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului are obligația de a asigura informarea publicului cu privire la existența situației prevăzute la alin. (1) cel puțin prin una dintre următoarele modalități:

a) prin intermediul unei secțiuni speciale pe pagina principală a propriei pagini de internet, cu menținerea acestei informări în aceste condiții cel puțin până la remedierea incidentului de securitate care are un impact semnificativ;

b) prin canalul propriu de televiziune;

c) prin intermediul poștei electronice;

d) prin intermediul serviciului de mesagerie scurtă;

e) prin mass-media.

(3) În cazul în care ANCOM nu a stabilit prin solicitarea prevăzută la alin. (2) modalitățile și condițiile pentru a se asigura informarea publicului, furnizorul de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului va realiza informarea cel puțin prin una dintre modalitățile prevăzute la alin. (2).

Art. 7. – Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului care au un număr de cel puțin 5.000 de utilizatori au obligația de a transmite ANCOM datele de contact ale persoanelor responsabile de notificarea inițială a incidentelor de securitate care au un impact semnificativ în conformitate cu dispozițiile art. 5, în termen de 5 zile de la intrarea în vigoare a prezentei decizii, precum și orice modificare a acestor date, în termen de 5 zile de la survenirea modificărilor.

Art. 8. – (1) În vederea creării unui cadru de cooperare în domeniul securității rețelelor și serviciilor de comunicații electronice se înființează Grupul consultativ pentru securitatea comunicațiilor electronice.

(2) Grupul prevăzut la alin. (1) are rol consultativ, va asigura o comunicare mai facilă și rapidă între ANCOM și furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pe diverse teme ce țin de domeniul securității rețelelor și serviciilor de comunicații electronice, identificarea unor soluții la probleme punctuale ce pot apărea, îmbunătățirea și promovarea continuă a securității rețelelor și serviciilor de comunicații electronice, diseminarea diverselor aspecte de securitate, inclusiv cele referitoare la incidente.

(3) Grupul prevăzut la alin. (1) este format din reprezentanți ai ANCOM și reprezentanți ai furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului care au un număr de cel puțin 100.000 de conexiuni. Un furnizor va fi reprezentat de cel puțin un expert tehnic în domeniu.

(4) Furnizorii menționați la alin. (3) vor desemna și vor comunica ANCOM datele de contact ale reprezentantului în Grupul prevăzut la alin. (1) în termen de 30 zile de la intrarea în vigoare a prezentei decizii, precum și orice modificare a acestor date, în termen de 5 zile de la survenirea acesteia.

(5) Prevederile prezentului articol nu se aplică furnizorilor de servicii de comunicații interpersonale care nu se bazează pe numere și furnizorilor de servicii de comunicații interpersonale bazate pe numere care nu exercită un control efectiv asupra transmiterii semnalului.

(6) La întâlnirile Grupului prevăzut la alin. (1) vor putea fi invitați să participe și reprezentanți ai altor entități - autorități, instituții publice, persoane juridice de drept public sau privat și asociații

de profil care reprezintă interesele furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, care nu îndeplinesc criteriile de la alin. (3).

Art. 9. – (1) Documentele prevăzute la art. 3 alin. (4) și (8), art. 4 alin. (7), art. 7, art. 8 alin. (4) transmise către ANCOM trebuie să fie semnate de reprezentantul legal al furnizorului, iar transmiterea se efectuează către adresa de poștă electronică securitate@ancom.ro, numai ca înscris în formă electronică, căruia i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv și generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

(2) Documentele prevăzute la art. 3 alin. (4) și (8) și art. 4 alin. (7) se vor transmite și în format editabil.

(3) Este considerată dată a transmiterii înscrisului în formă electronică data confirmării primirii de către ANCOM a acestui înscris. ANCOM asigură fără întârziere și în mod automat confirmarea primirii înscrisului în formă electronică transmis la adresa de poștă electronică prevăzută la alin. (1).

(4) În situația în care confirmarea primirii unui înscris în formă electronică nu s-a realizat în condițiile alin. (3), este considerată dată a transmiterii data la care înscrisul în formă electronică a fost primit, astfel cum este aceasta atestată de calculatorul de primire al ANCOM.

Art. 10. – Anexele nr. 1 - 3 fac parte integrantă din prezenta decizie.

Art. 11. – (1) Prezenta decizie se publică în Monitorul Oficial al României, Partea I, și intră în vigoare la data publicării, cu excepția prevederilor art. 3, care intră în vigoare în termen de 3 luni de la data publicării prezentei decizii în Monitorul Oficial al României, Partea I, și a prevederilor art. 4, care intră în vigoare în termen de 18 luni de la data publicării prezentei decizii în Monitorul Oficial al României, Partea I.

(2) La data intrării în vigoare a prezentei decizii, Decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații nr. 512/2013 privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, publicată în Monitorul Oficial al României, Partea I, nr. 517 din 19 august 2013, se abrogă, cu excepția prevederilor art. art. 3 alin. (1), (3) și (4) și ale anexei nr. 1, care își vor înceta aplicabilitatea la data intrării în vigoare a prevederilor art. 3 din prezenta decizie.

PREȘEDINTE,

Valeriu Ștefan ZGONEA

București, 1 februarie 2024.

Nr. 70.

DOMENIILE

vizate de măsurile de securitate

Domeniul I. Politica de securitate și managementul riscului

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului 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, amenințărilor, vulnerabilităților, măsurilor existente și a consecințelor pe care incidentele de securitate le-ar putea avea asupra resurselor și să se asigure că personalul de conducere este informat în mod corespunzător despre aceste riscuri, dar și despre măsurile de reducere a lor; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G, se vor avea în vedere, totodată, potențiale riscuri cauzate de expunerea la terțe părți considerate a prezenta un grad de risc ridicat ori dependența de un singur producător;
 - c) să analizeze riscurile prin estimarea impactului pe care îl poate avea concretizarea unei amenințări care exploatează o vulnerabilitate a unei resurse și prin estimarea 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;
 - f) să se asigure că riscurile reziduale sunt acceptate de personalul de conducere;
3. să stabilească o structură adecvată a rolurilor și responsabilităților în asigurarea securității rețelelor și serviciilor, să informeze personalul despre rolurile și responsabilitățile în asigurarea securității rețelelor și serviciilor, precum și despre cazurile și modalitățile în care se pot contacta persoanele responsabile;
4. să stabilească o politică cu privire la cerințele de securitate atât pentru achiziționarea de produse și servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate (echipamente, servicii IT, software, interconectare, baze de date, facilități asociate etc.), cât și pentru asigurarea întreținerii sau gestiunii de către terțe părți a acestor produse și servicii;
5. să includă cerințe de securitate în contractele pentru achiziționarea de la terțe părți de produse și servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate și pentru asigurarea întreținerii sau gestiunii de către terțe părți a acestor produse și servicii, inclusiv în ceea ce privește confidențialitatea și transferul securizat al informației, să țină evidența incidentelor de securitate cauzate de terțe părți, să ia măsuri pentru a reduce riscurile reziduale care nu au fost adresate de terțele părți sau sunt rezultate din interacțiunea cu acestea;

6. În ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să includă în politica privind cerințele de securitate pentru achiziționarea de la terțe părți de produse și servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate și pentru asigurarea întreținerii sau gestiunii de către terțe părți a acestor produse și servicii cel puțin următoarele elemente:

- a) referitor la echipamentele identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, obligația achiziționării unor echipamente puse la dispoziție de terțele părți, precum și a proceselor și serviciilor acestora [procese TIC, servicii TIC, produse TIC, echipamente din componența rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, servicii cloud etc.] certificate în conformitate cu sistemele europene de certificare aplicabile, în cazul în care astfel de sisteme de certificare prevăzute de Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) sunt obligatorii în temeiul dreptului național sau european;
- b) obligația de a depune diligențele necesare pentru a se asigura că terții respectă standardele relevante în proiectarea și fabricarea echipamentelor, precum și în gestionarea ciclului de viață al acestora;
- c) prezentarea documentelor justificative de către terți care să ateste că aceștia au depus diligențele necesare în vederea asigurării nivelului de calitate al proceselor interne de securitate aplicabile, inclusiv asigurarea securității prin proiectare (*security by design*), integrată în procesul de dezvoltare a produsului;
- d) furnizarea de către terți a garanțiilor și documentelor justificative care să ateste că aceștia au depus diligențele necesare în ceea ce privește implementarea tuturor funcționalităților de securitate conform standardelor relevante și că în produsele pe care le pun la dispoziție nu există vulnerabilități introduse și/sau omise voit; aceștia vor informa imediat despre vulnerabilități de îndată ce acestea devin cunoscute;
- e) obligația de a depune diligențele necesare pentru a se asigura că terții asigură protecția adecvată și nedivulgarea oricăror informații confidențiale despre beneficiarii echipamentelor, serviciilor, lucrărilor sau a altor informații confidențiale către alte entități;
- f) obligația de a depune diligențele necesare pentru a se asigura că terții vor oferi asistență în investigarea și remedierea incidentelor de securitate și posibilitatea de a colabora în vederea efectuării unor eventuale teste periodice de securitate și de penetrare ale produselor pe care le pun la dispoziție.

Domeniul II. Securitatea resurselor umane

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

1. să stabilească un proces privind verificarea de fond a candidaților pentru angajare, a contractorilor și a terților în conformitate cu legile aplicabile, reglementări și etică, proporționale cu riscurile percepute, și să efectueze, în baza procesului menționat, controale de verificare de fond a candidaților pentru angajare, a contractorilor și a terților;
2. să se asigure că personalul are cunoștințe suficiente de securitate și este instruit permanent cu privire la securitatea rețelelor și serviciilor, inclusiv prin implementarea unor programe de instruire

regulată în domeniul securității rețelelor și serviciilor de comunicații electronice, precum și să pună la dispoziția personalului materiale și documentații suport actualizate;

3. să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri și responsabilități, care să cuprindă inclusiv aspecte privind revocarea drepturilor de acces, predarea echipamentelor dacă nu mai sunt necesare, precum și instruirea personalului în cazul schimbărilor responsabilităților în cadrul organizației;

4. să stabilească un proces disciplinar pentru angajații care produc o încălcare a securității rețelelor sau serviciilor de comunicații electronice.

Domeniul III. Securitatea rețelelor și serviciilor, a facilităților asociate și a informațiilor

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

1. să stabilească o securitate fizică și de mediu adecvată a rețelei și a facilităților asociate, care să includă: stabilirea și menținerea unor măsuri de securitate 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. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să stabilească măsuri de securitate suplimentare pentru accesul fizic la rețea și la facilitățile asociate, în conformitate cu importanța obiectivului protejat; măsurile de securitate vor ține cont de riscurile specifice acestor rețele, inclusiv cele generate de accesul părților terțe;

3. să stabilească o securitate adecvată a utilităților suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor, cel puțin prin: implementarea unor măsuri prin care să se asigure securitatea adecvată a utilităților suport, dar și a facilităților conexe, proiectarea și dimensionarea acestora astfel încât să fie în acord cu cerințele și specificațiile producătorilor de echipamente;

4. să stabilească măsuri de securitate adecvate pentru accesul logic la rețea și la sistemele informatice, care să prevadă cel puțin:

- a) implementarea unor mecanisme de control al accesului logic pe baza unor identificatori unici;
- b) managementul drepturilor de acces, definirea rolurilor, a drepturilor de acces și a responsabilităților, mecanismele de autentificare adecvate tipului de acces solicitat, precum și monitorizarea accesului, procese privind aprobarea excepțiilor și înregistrarea fraudelor;
- c) măsuri de securitate privind accesul logic al terților, de la distanță, la resurse, aplicarea principiului „privilegiilor minime”, a principiului „separării sarcinilor”, monitorizarea continuă a accesului, aplicarea autentificării bazate pe tehnologii de ultimă generație.

5. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, se vor implementa măsuri de securitate suplimentare pentru accesul logic care vor ține cont de riscurile specifice ale acestor rețele. Controlul strict al accesului și/sau restricționarea accesului vor fi avute în vedere în cazul terților sau furnizorilor de servicii gestionate (entitățile care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță) care sunt considerați de risc ridicat sau care accesează din țări din afara Uniunii Europene rețelele și sistemele informatice;

6. 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, malware;
7. să aplice măsuri de securitate adecvate în cazul managementului actualizărilor, corecțiilor software, dar și în cazul traficului de management și de semnalizare, în vederea prevenirii intervențiilor neautorizate în cadrul rețelei sau componentelor acesteia;
8. să asigure utilizarea adecvată a criptării datelor în timpul stocării sau a transmiterii lor prin rețea pentru a preveni incidentele de securitate și/sau pentru a minimiza impactul acestora asupra utilizatorilor finali sau a altor rețele sau servicii de comunicații electronice;
9. să asigure protecția adecvată a cheilor criptografice și a oricăror altor informații de autentificare pentru a nu fi divulgate sau alterate, iar accesul la cheile private să fie monitorizat și controlat.

Domeniul IV. Managementul operațiunilor

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

1. să stabilească proceduri operaționale și responsabilități adecvate și să se asigure că toate sistemele necesare furnizării rețelelor și serviciilor de comunicații electronice sunt gestionate conform acestor proceduri operaționale;
2. să stabilească proceduri privind managementul schimbărilor efectuate în rețeaua de comunicații electronice, inclusiv schimbările software, și să se asigure că acestea sunt realizate conform procedurilor adoptate;
3. să întocmească și să păstreze cel puțin un an jurnale care să conțină informațiile relevante referitoare la schimbările de la pct. 2, inclusiv în cazul schimbărilor software (evidența schimbărilor, a corecțiilor, a actualizărilor etc.);
4. să efectueze evaluări prelabile ale impactului potențial al unei schimbări de sistem;
5. să stabilească proceduri de gestionare a resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate și controlul configurării astfel încât disponibilitatea și starea acestora să fie verificată, care să includă:
 - a) identificarea și inventarierea resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, inclusiv cele ale unor terțe părți, întocmirea de registre actualizate care să conțină detalii despre tehnologiile și componentele puse în funcțiune, dependența între aceste resurse, precum și identificarea configurărilor sistemelor;
 - b) stabilirea proprietarilor resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, definirea rolurilor, responsabilităților;
 - c) evaluarea de criticitate a resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate bazată pe evaluarea de risc.

Domeniul V. Managementul incidentelor

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

1. să stabilească procese și proceduri pentru managementul incidentelor care afectează securitatea rețelelor și serviciilor de comunicații electronice care să vizeze raportarea internă, evaluarea, răspunsul la incidente și escaladarea acestora, inclusiv prin definirea rolurilor și responsabilităților;
2. să se asigure de pregătirea adecvată, existența și disponibilitatea personalului pentru managementul incidentelor care afectează securitatea rețelelor și serviciilor de comunicații electronice;
3. să stabilească și să implementeze procese și sisteme de detectare a incidentelor de securitate și a evenimentelor care pot conduce la incidente;
4. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, centrele de operațiuni de rețea și/sau centrele de operațiuni de securitate vor funcționa pe teritoriul național și/sau pe teritoriul Uniunii Europene; acestea ar trebui să asigure vizibilitatea și monitorizarea componentelor rețelei respective pentru a detecta evenimente de securitate și pentru a identifica și preveni amenințări;
5. să stabilească o procedură adecvată de raportare a incidentelor către Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), precum și către alte autorități responsabile și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori de rețele și servicii de comunicații electronice afectați, media, clienți, parteneri de afaceri etc.);
6. să stabilească procese și proceduri pentru restabilirea prioritară a serviciilor ce contribuie la realizarea comunicațiilor de urgență.

Domeniul VI. Managementul continuității afacerii

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului 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; aceasta va include și măsuri privind asigurarea rezilienței lanțului de aprovizionare cu echipamente și software necesare furnizării rețelelor și serviciilor de comunicații;
2. să dețină capacități de implementare a strategiei de continuitate și să stabilească planuri de continuitate și de recuperare;
3. în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, planurile de continuitate și de recuperare să aibă în vedere suplimentar:
 - dependența de alte sectoare și servicii critice a căror afectare poate impacta direct sau indirect securitatea rețelelor și serviciilor;
 - afectarea altor sectoare și servicii critice dependente de continuitatea furnizării rețelelor și serviciilor de comunicații electronice;
4. să stabilească o strategie pentru asigurarea accesului neîntrerupt la comunicațiile de urgență.

Domeniul VII. Monitorizare, testare și audit

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

1. să stabilească politici de monitorizare a sistemelor, precum și politici privind jurnalele de sistem care să asigure vizibilitate adecvată, să detecteze anomalii, să identifice și să prevină amenințări, inclusiv în ceea ce privește asigurarea comunicațiilor de urgență;
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, având în vedere scenarii realiste care să acopere cât mai multe situații posibile; în urma analizei rezultatelor vor fi luate măsurile corespunzătoare;
3. să stabilească politici pentru testarea echipamentelor, sistemelor, software-lor și corecțiilor software înainte de conectarea/punerea lor în funcțiune/implementarea lor;
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; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, politica pentru monitorizarea conformității va cuprinde aplicarea măsurilor de securitate din standardele relevante.

Domeniul VIII. Conștientizarea amenințărilor

Obiective de securitate

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

1. să stabilească și să implementeze procese de monitorizare, colectare și analiză continuă a informațiilor despre amenințările relevante la adresa securității rețelelor și serviciilor de comunicații electronice;
2. să ia măsuri adecvate de atenuare și prevenire a amenințărilor relevante la adresa securității rețelelor și serviciilor de comunicații electronice.

FORMULAR DE RAPORTARE
a incidentelor cu impact semnificativ asupra rețelelor și serviciilor de comunicații
electronice (disponibilitate, confidențialitate, integritate sau autenticitate)

1. Furnizor:

2. Data și ora:

- Data și ora la care s-a produs incidentul — data: ora:
- Data și ora la care s-a descoperit incidentul — data: ora:

3. Dimensiunea afectată a securității:

- disponibilitate;
- autenticitate;
- integritate;
- confidențialitate.

4. Incidentul este repetitiv:

- Da (specificați data ultimei apariții):
- Nu.

5. Pragurile depășite:

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

6. Impactul incidentului:

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

7. Descrierea incidentului:

8. Acțiunile de răspuns:

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

10. Alți furnizori de rețele și servicii de comunicații electronice afectați:

Da (specificați numele furnizorului/furnizorilor.):

Nu.

11. Persoana de contact:

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

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

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

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

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

6. Impactul incidentului

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

7. Descrierea incidentului

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

8. Acțiunile de răspuns

Câmpul va cuprinde măsurile de securitate implementate până la momentul producerii incidentului și descrierea detaliată a acțiunilor de răspuns, inclusiv momentele în care au fost acestea realizate. Spre exemplu, se vor detalia acțiunile întreprinse pentru a aduce serviciul la un nivel acceptabil, precum și pentru a restabili serviciul la parametrii inițiali, în cazul afectării disponibilității, acțiunile întreprinse în ceea ce privește limitarea pierderii suplimentare a datelor, evaluarea pierderilor survenite prin colectarea faptelor și evaluarea riscurilor, inclusiv a potențialelor prejudicii aduse persoanelor afectate, în cazul afectării autenticității, integrității sau confidențialității. Se vor menționa alte autorități care au fost contactate și acțiunile de informare a persoanelor implicate în incident, dacă este cazul.

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

Câmpul va cuprinde descrierea detaliată a acțiunilor realizate pentru a minimiza nivelul de risc și pentru a preîntâmpina reparația incidentului (de exemplu, revizuire măsuri de securitate și proceduri, renegociere SLA-uri, instruirii de personal, achiziție de echipamente sau sisteme de backup etc.), precum și momentul când au fost luate sau când vor fi luate aceste măsuri. Acest câmp va conține și informații despre lecțiile învățate - aceasta presupune realizarea unui bilanț al incidentului, ajungerea la sursa problemei (root cause), cum și de ce s-a întâmplat, evaluarea a cât de bine a funcționat planul de răspuns la incident pentru a rezolva problema și identificarea îmbunătățirilor care trebuie făcute.

10. Alți furnizori de rețele și servicii de comunicații electronice afectați

Se va bifa una dintre cele 2 opțiuni. În situația în care sunt afectați și alți furnizori, se vor specifica denumirile furnizorilor afectați de incidentul în cauză.

11. Persoana de contact

Se vor indica datele de contact ale persoanei responsabile (nume, prenume, număr telefon de contact, e-mail) cu furnizarea clarificărilor de natură tehnică, în cazul în care va fi nevoie.