DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Ghid privind elaborarea politicii pentru rețelele private virtuale (VPN)

IULIE 2026

TLP:CLEAR

Cuprins

1. Introducere

În această secțiune se va preciza contextul, scopul și importanța protejării accesului la resursele și informațiile organizației. Se recomandă includerea unei referiri la tipul de date gestionate și la riscurile specifice domeniului de activitate.

Rețelele private virtuale (VPN) sunt esențiale pentru protejarea comunicațiilor realizate prin rețele nesigure, inclusiv prin intermediul internetului public. Ele asigură confidențialitatea, integritatea și autenticitatea datelor, reduc aria de expunere și controlează accesul la resursele organizației.

Organizațiile prelucrează și dețin categorii variate de informații sensibile precum: date cu caracter personal, informații confidențiale contractuale, date financiare, proprietate intelectuală, secrete comerciale și, după caz, informații clasificate. Compromiterea oricăreia dintre aceste categorii prin canale de comunicare neprotejate poate genera prejudicii semnificative: sancțiuni legale, pierderi financiare, deteriorarea relațiilor contractuale sau afectarea reputației.

Ordonanța de urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, care transpune Directiva (UE) 2022/2555 (NIS2), aprobată prin Legea nr. 124/2025, impune entităților esențiale și importante să adopte măsuri tehnice, operaționale și organizatorice adecvate pentru protecția rețelelor și sistemelor informatice, inclusiv securizarea accesului la distanță. Totodată, Regulamentul (UE) 2016/679 (GDPR) impune obligații clare privind protejarea datelor cu caracter personal, inclusiv în contextul accesului la distanță și al transmiterii acestora prin rețele externe.

Prezentul ghid reprezintă un element esențial al cadrului de securitate cibernetică al organizației și:

- stabilește cadrul formal prin care organizația reglementează utilizarea conexiunilor VPN pentru accesul la distanță și pentru conectarea securizată între locații;
- definește responsabilitățile și cerințele tehnice aplicabile soluțiilor VPN utilizate;
- asigură conformitatea cu obligațiile legale și cu standardele internaționale în materie de securitate a comunicațiilor;
- minimizează riscul interceptării, accesului neautorizat și scurgerii de date prin rețele nesigure.

2. Domeniu de aplicare

În această secțiune se vor preciza categoriile de sisteme, persoanele și dispozitivele asupra cărora se aplică prevederile politicii, respectiv eventualele excepții. Se va acorda atenție identificării situațiilor în care organizația utilizează conexiuni la distanță pentru accesarea resurselor interne.

Politica VPN se aplică tuturor sistemelor, dispozitivelor și conexiunilor prin care resursele informatice ale organizației sunt accesate prin rețele externe, indiferent de suportul utilizat (laptop, telefon mobil, tabletă, dispozitiv personal) și de locația din care se realizează accesul (biroul de acasă, deplasări, locații ale partenerilor, spații publice).

Aplicarea prevederilor politicii este obligatorie pentru toți cei care accesează, prelucrează sau gestionează informațiile organizației prin rețele externe, inclusiv:

- angajați care lucrează de la distanță sau în regim hibrid;
- colaboratori externi și contractori cu acces la sistemele interne;
- furnizori care asigură administrarea sau suportul tehnic de la distanță.

Politica este în concordanță cu politica de răspuns la incidente de securitate cibernetică[1] a organizației și cu celelalte politici de securitate adoptate. Acestea se aplică concomitent și complementar: Politica de răspuns la incidente guvernează reacția tehnică la orice incident de securitate, în timp ce Politica VPN reglementează condițiile și cerințele tehnice în care accesul la distanță este permis, astfel încât riscul producerii unui incident să fie redus la minimum.

[1] Ghid pentru elaborarea politicii de răspuns la incidente de securitate cibernetică, disponibil la: https://www.dnsc.ro/vezi/document/dnsc-bune-practici-pentru-elaborarea-unei-politici-de-raspuns-la-incidente-de-securitate-cibernetica, accesat 29.06.2026.

Excluderi: Conexiunile realizate exclusiv în rețeaua locală (LAN) a organizației, fără traversarea unor rețele externe, nu fac obiectul prezentului ghid.

3. Cadru legal și normativ aplicabil

Elaborarea politicii interne de utilizare VPN de către organizație are în vedere respectarea cadrului legal european și național, precum și a standardelor internaționale relevante pentru securitatea comunicațiilor și protecția datelor.

3.1 Legislația europeană

- Directiva (UE) 2022/2555 (NIS2) privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniunea Europeană stabilește obligații de gestionare a riscurilor, inclusiv utilizarea conexiunilor securizate și protecția rețelelor și sistemelor informatice;
- Regulamentul (UE) 2016/679 (GDPR) impune implementarea de măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal, inclusiv criptarea comunicațiilor și securizarea accesului la distanță;
- Regulamentul (UE) 2019/881 (Cybersecurity Act) stabilește cadrul european de certificare a securității cibernetice, fiind relevant pentru selecția soluțiilor VPN certificate la nivel european.

3.2 Legislația națională

- OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, care transpune Directiva NIS2, aprobată prin Legea nr. 124/2025, stabilește obligații concrete pentru entitățile esențiale și importante, inclusiv securizarea accesului la distanță și gestionarea riscurilor de rețea;
- Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR la nivel național.

3.3 Standarde și bune practici internaționale

- ISO/IEC 27001:2022 - sisteme de management al securității informației: controlul accesului, criptarea comunicațiilor, securitatea rețelelor;
- ISO/IEC 27002:2022 - ghid de bune practici pentru controale de securitate: acces la rețea, autentificare, criptare;
- ISO/IEC 27033 - securitatea rețelelor, inclusiv proiectarea și implementarea soluțiilor VPN;
- NIST SP 800-77 Rev. 1 - Guide to IPsec VPNs: ghid tehnic actualizat pentru implementarea VPN pe baza protocolului IPsec;
- NIST SP 800-46 Rev. 2 - Guide to Enterprise Telework and Remote Access Security: ghid complet pentru securizarea accesului la distanță în medii enterprise.

4. Roluri și responsabilități

Gestionarea eficientă a soluției VPN depinde de o definire clară a rolurilor și responsabilităților. Se recomandă ca toate persoanele cu atribuții în implementarea și monitorizarea VPN să fie desemnate nominal, să primească o copie a politicii interne și să fie instruite periodic. Datele de contact ale responsabililor se actualizează ori de câte ori intervin modificări.

- Departamentul IT / Administratorii de sistem configurează, administrează și monitorizează soluția VPN; aplică actualizările de securitate periodic; gestionează conturile de acces VPN și revocă accesul la cerere sau la încetarea relației contractuale.
- CISO / Responsabilul cu Securitatea Cibernetică validează și aprobă politica internă de utilizare VPN a organizației; coordonează implementarea și conformitatea; aprobă excepțiile pe baza unei analize de risc documentate; primește rapoartele de incident legate de VPN.
- Structura responsabilă cu securitatea informațiilor diseminează politica internă tuturor utilizatorilor, în colaborare cu Departamentul HR; asigură instruirea periodică a utilizatorilor.
- Conducerea organizației aprobă politica internă de utilizare VPN și asigură resursele necesare implementării și menținerii soluției.

- Utilizatorii finali utilizează soluția VPN în conformitate cu politicile interne ale organizației, raportează imediat orice incident sau comportament anormal al conexiunii VPN și nu divulgă niciunei persoane neautorizate credențialele de acces.

5. Cerințe tehnice privind infrastructura VPN

Cerințele tehnice stabilite (protocoale moderne, algoritmi puternici, chei adecvate) sunt necesare pentru a asigura un nivel ridicat de securitate și pentru a preveni atacurile asupra conexiunilor VPN. Protocoalele și algoritmii vechi pot fi vulnerabili, de aceea sunt excluși. Autentificarea multi-factor și monitorizarea conexiunilor reduc riscul accesului neautorizat și ajută la detectarea incidentelor.

Specificațiile tehnice se adaptează în funcție de soluția adoptată și de recomandările furnizorului, asigurând alinierea cu NIST SP 800-77 Rev. 1 și ISO/IEC 27033.

5.1 Procesul de selecție, evaluare și aprobare a soluției VPN

Orice soluție VPN utilizată în cadrul organizației se aprobă în prealabil de CISO și de Departamentul IT. Criteriile de selecție includ:

- suportul pentru protocoale criptografice moderne;
- disponibilitatea actualizărilor de securitate și politica de suport a furnizorului;
- compatibilitatea cu infrastructura existentă și cu cerințele de autentificare;
- existența documentației tehnice clare și a unui istoric de audit de securitate;
- conformitatea cu standardele de certificare relevante (ISO/IEC 27001, Cybersecurity Act UE).

5.2 Protocoale și algoritmi de criptare

Soluțiile VPN utilizate în cadrul organizației folosesc exclusiv protocoale și algoritmi criptografici considerați siguri conform NIST SP 800-77 Rev. 1.

Sunt acceptate:

- protocoale VPN: IPsec/IKEv2 (recomandat), OpenVPN (TLS 1.2+), WireGuard; SSL VPN (bazat pe TLS 1.2 / TLS 1.3);[2]
- algoritmi de criptare simetrică: AES-256-GCM (recomandat), AES-128-GCM (minim acceptat);
- algoritmi de schimb de chei: ECDH (P-256 sau P-384), DHE cu parametri de minim 3072 biți;
- funcții hash: SHA-256 (minim), SHA-384 sau SHA-512 (recomandat);
- certificate digitale: RSA 3072+ biți sau ECC P-256+, emise de o Autoritate de Certificare de încredere.

Sunt interzise:

- protocoale de tunel: PPTP, L2TP fără IPsec;
- versiuni SSL/TLS: orice versiune sub TLS 1.2;
- algoritmi de criptare: DES, 3DES, RC4;
- algoritmi de hashing: MD5, SHA-1;
- schimb de chei: grupuri Diffie-Hellman sub 2048 biți.

5.3 Autentificarea și controlul accesului

Accesul la infrastructura VPN este permis exclusiv pe baza autentificării cu factori multipli (MFA). Se recomandă implementarea:

- autentificării cu minim doi factori: parolă + token TOTP / certificat digital / card inteligent;
- integrării cu integrării cu baza de date a utilizatorilor (Active Directory / LDAP);

[2] Deși SSL VPN este cel mai folosit tip de VPN pentru acces de la distanță în mediile enterprise și este relativ simplu de implementat pentru controlul accesului și RBAC, acesta este și cel mai frecvent vizat de atacatori. În ultimii ani, majoritatea vulnerabilităților și atacurilor care au afectat soluțiile VPN au fost concentrate pe implementările SSL VPN, deoarece expun direct servicii accesibile din internet și folosesc componente complexe care pot conține erori exploatabile.

- politicii de parolă aliniată cu standardele organizației (lungime minimă, complexitate, rotație periodică);[3]
- blocării automate a contului după un număr prestabilit de tentative eșuate de autentificare;
- revocării imediate a accesului VPN la încetarea relației contractuale sau la cererea CISO.

5.4 Tunelare divizată (Split tunneling)

Tunelarea divizată (Split Tunneling) permite utilizatorilor să acceseze resurse locale simultan cu o conexiune VPN, ocolind parțial controalele de securitate. Organizația decide explicit dacă această funcționalitate este permisă sau interzisă și documentează decizia.

Este permisă ca opțiune implicită în cadrul organizației pentru utilizatorii obișnuiți, cu scopul de a proteja banda de internet a organizației de traficul personal al angajaților. Configurarea se realizează exclusiv de Departamentul IT. Prin excepție, full tunneling (interzicerea split tunneling) este obligatoriu și se aplică strict pentru conturile cu drepturi critice (ex. administratori), unde inspecția totală a traficului este obligatorie.

Organizațiile care optează pentru interzicerea completă a tunelării vor configura full tunneling pentru toți utilizatorii, direcționând tot traficul prin controalele de securitate interne.

5.5 Conexiuni VPN între locații (site-to-site)

Conexiunile VPN permanente între locațiile organizației, precum și cele stabilite cu parteneri sau furnizori terți, se implementează pe baza:

- unui acord tehnic documentat (specificații tunel, protocoale, adrese IP agreate);
- autorizării formale din partea CISO și a managementului;
- unui acord de securitate cu partenerul sau furnizorul (clauze contractuale privind cerințele de securitate cibernetică);
- monitorizării traficului și revizuirii periodice a necesității conexiunii.

5.6 Clienți VPN și dispozitive terminale

Pe dispozitivele utilizate pentru conexiunea VPN se respectă cumulativ următoarele cerințe:

- utilizarea exclusivă a aplicației VPN aprobate de organizație;
- actualizarea sistemului de operare, cu toate patch-urile de securitate aplicate;
- menținerea unei soluții antivirus/EDR active și actualizate.

Organizațiile vor lua măsuri în vederea tranziției către modelul Zero Trust Network Access (ZTNA), prin implementarea verificării posturii dispozitivului (Endpoint Posture Check) - un mecanism care validează automat starea de securitate a dispozitivului terminal înainte de deschiderea tunelului VPN. Prin adoptarea acestui model, accesul nu mai este acordat exclusiv pe baza credențialelor, ci condiționat de îndeplinirea unor criterii de securitate verificabile: sistem de operare actualizat, soluție antivirus activă și conformitate cu politicile organizației.

Dispozitivele personale (BYOD) pot fi utilizate pentru acces VPN numai dacă respectă politica BYOD a organizației și sunt înrolate în soluția MDM aprobată.

6. Gestionarea accesului VPN

6.1 Gestionarea drepturilor de acces

Accesul VPN se acordă pe baza principiului minimului necesar și al necesității operaționale, printr-un proces care include:

- solicitarea formală din partea managerului direct al utilizatorului;
- aprobarea CISO;

[3] Conform ghidurilor moderne NIST, se recomandă eliminarea rotației periodice forțate a parolelor (ex: la 90 de zile) dacă este implementat MFA obligatoriu, schimbarea făcându-se doar la suspiciunea de compromitere. Totuși, dacă instituția are deja o politică internă mai strictă (ex: schimbare la 6 luni), aceasta va prevala.

- configurarea tehnică de către Departamentul IT, cu activarea MFA;
- confirmarea scrisă de luare la cunoștință a politicii interne din partea utilizatorului.

6.2 Revizuirea periodică a accesului

Drepturile de acces VPN se revizuiesc periodic de Departamentul IT, cu aprobarea managerilor de departament. Accesul care rămâne inactiv peste un interval prestabilit este revocat automat, iar CISO este informat pentru a aproba fie reactivarea, fie eliminarea permanentă a acestuia.

6.3 Revocarea accesului

Accesul VPN este revocat imediat în următoarele situații:

- încetarea relației de muncă sau a contractului cu colaboratorul/terțul;
- schimbarea rolului care nu mai necesită acces la distanță;
- suspendarea disciplinară sau la cererea CISO;
- pierderea, furtul sau compromiterea dispozitivului utilizat pentru VPN;
- detectarea unui incident de securitate asociat contului.

7. Monitorizare și jurnalizare

Toate sesiunile VPN sunt monitorizate și jurnalizate automat. Jurnalele conțin cel puțin:

- identitatea utilizatorului (ID utilizator);
- adresa IP, sursă și destinație;
- data și ora conectării/deconectării și durata sesiunii;
- volumul de date transferat;
- rezultatul autentificării (succes / eșec);
- dispozitivul utilizat (dacă este disponibil tehnic).

Jurnalele sunt stocate centralizat și sunt protejate împotriva modificării neautorizate. Perioada de retenție se stabilește de fiecare organizație în parte, cu respectarea principiilor GDPR privind limitarea stocării și a politicii interne de retenție a datelor. Se recomandă un minim de 12 luni.

Sistemul de monitorizare generează alerte automate în cazul:

- tentativelor repetate de autentificare eșuată;
- conectărilor din locații geografice neobișnuite sau simultan din locații diferite;
- transferului unui volum neobișnuit de mare de date;
- conectărilor în afara orelor normale de lucru, fără justificare documentată;
- utilizării de protocoale sau clienți neautorizați.

Utilizatorii sunt informați explicit, prin politica internă și prin notificarea de confidențialitate a organizației, că sesiunile VPN sunt monitorizate în scopuri de securitate cibernetică.

8. Gestionarea incidentelor legate de VPN

Constituie incident de securitate VPN orice eveniment care implică sau poate implica acces neautorizat, credențiale compromise, comportament anormal al sesiunii sau pierderea/furtul unui dispozitiv cu client VPN instalat. Orice astfel de eveniment se raportează imediat prin canalul oficial de raportare a incidentelor al organizației.

La momentul detectării unui incident, Departamentul IT declanșează următoarele măsuri:

- suspendarea imediată a contului VPN afectat;
- izolarea dispozitivului implicat (dacă este posibil tehnic);
- colectarea și conservarea jurnalelor pentru investigație;

- notificarea CISO și demararea investigației de securitate;
- evaluarea impactului și aplicarea măsurilor de remediere.

CISO sau persoana desemnată de acesta are responsabilitatea de a raporta incidentele de securitate cibernetică către Directoratul Național de Securitate Cibernetică (DNSC), în termenele prevăzute de OUG nr. 155/2024 și Legea nr. 124/2025, fără întârzieri nejustificate.

9. Testare, audit și îmbunătățire continuă

9.1 Verificări periodice

Tabel 1 – Tipuri de verificare

Tip verificare	Frecvență	Responsabil
revizuire configurații VPN (protocoale, criptare, reguli de acces)	semestrial	Departament IT/ securitate
scanare vulnerabilități pe componente VPN	trimestrial	Departament IT / securitate
test de penetrare (pentest) - inclusiv infrastructura VPN	anual	Furnizor extern autorizat
revizuire jurnale și alerte SIEM	lunar	CISO / SOC
revizuire liste de acces (conturi active, drepturi)	trimestrial	Departament IT + manageri departamente

9.2 Actualizare și revizuire

Politica VPN se revizuiește și se actualizează:

- anual, în mod planificat;
- după orice incident de securitate major care a implicat infrastructura VPN;
- la apariția unor modificări legislative sau normative relevante;
- la schimbări semnificative ale infrastructurii tehnice sau ale modelului de lucru al organizației.

Versiunile depășite sunt arhivate și păstrate pentru referință.

10. Instruire și conștientizare

Toți utilizatorii cu acces VPN se vor instrui cu privire la:

- regulile de utilizare a VPN conform politicii interne a organizației;
- riscurile utilizării rețelelor publice fără VPN;
- recunoașterea și raportarea tentativelor de phishing care vizează credențialele VPN;
- procedura de raportare a incidentelor și a dispozitivelor pierdute/furate.

Instruirea este obligatorie la acordarea accesului VPN (cu confirmare scrisă) și se repetă anual sau în cazul în care apar modificări semnificative ale politicii.

11. Încălcarea prevederilor politicii

Nerespectarea politicii interne de utilizare VPN atrage măsuri disciplinare în conformitate cu legislația în vigoare și regulamentele interne ale organizației. Încălcările cu caracter penal sau care implică scurgeri de date cu caracter personal se raportează autorităților competente (ANSPDCP, MAI după caz).

12. Dispoziții finale

Politica va intra în vigoare imediat după aprobarea sa de către conducerea organizației. Orice revizuire ulterioară se supune aceluiași proces de aprobare și înlocuiește integral versiunea precedentă.

13. Termeni și definiții

Termen	Definiție
AES-256-GCM	Advanced Encryption Standard cu cheie de 256 biți în modul Galois/Counter Mode - algoritm de criptare simetrică recomandat conform standardelor actuale NIST.
BYOD (Bring Your Own Device)	Politică prin care angajații utilizează dispozitive personale pentru activități profesionale.
CISO	Chief Information Security Officer - responsabilul cu securitatea informațiilor / cibernetică din cadrul organizației sau funcția echivalentă.
CVE (Common Vulnerabilities and Exposures)	Sistem standardizat de identificare și catalogare publică a vulnerabilităților de securitate cunoscute.
EDR (Endpoint Detection and Response)	Soluție de securitate care monitorizează dispozitivele, detectează activități malițioase și permite răspuns rapid la incidente.
EPC (Endpoint Posture Check)	Verificare automată a stării de securitate a unui dispozitiv înainte de acordarea accesului la resursele organizației.
Full tunneling	Configurație VPN în care tot traficul utilizatorului este direcționat prin tunelul VPN și prin controalele de securitate ale organizației.
IKEv2 (Internet Key Exchange version 2)	Protocol pentru negocierea cheilor criptografice utilizat în VPN-urile IPsec.
Incident de securitate cibernetică	Eveniment survenit în spațiul cibernetic care perturbă funcționarea unuia sau mai multor sisteme informatice și ale cărui consecințe pot afecta securitatea cibernetică (conform OUG nr. 155/2024).
IPsec (Internet Protocol Security)	Suită de protocoale pentru autentificarea și criptarea pachetelor IP la nivelul rețelei.
MDM (Mobile Device Management)	Soluție software pentru gestionarea centralizată a dispozitivelor mobile utilizate în mediul organizațional.
MFA (Multi-Factor Authentication)	Autentificare cu factori multipli - metodă de verificare a identității utilizând cel puțin doi factori distincți (ex. parolă + token).
SIEM (Security Information and Event Management)	Sistem centralizat de colectare, corelare și analiză a jurnalelor și evenimentelor de securitate.
Split tunneling	Configurație VPN în care numai o parte a traficului utilizatorului este direcționat prin tunelul VPN, restul mergând direct spre internet.

TLS (Transport Layer Security)	Protocol criptografic pentru asigurarea comunicațiilor securizate; înlocuiește protocolul SSL.
VPN (Virtual Private Network)	Rețea privată virtuală - tehnologie care creează un tunel criptat pentru comunicații securizate prin rețele nesigure (ex. internet public).
ZTNA (Zero Trust Network Access)	Model de securitate care acordă accesul la resurse exclusiv pe baza verificării continue a identității și a stării dispozitivului, fără a acorda încredere implicită niciunui utilizator sau locații.

Autori: **Andrei Dodițe, Vlad Drăguș, Cristina Cristina**

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.