					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P21					Titlul documentului: **Politica de securitate a rețelei**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 8	N/A
ISO/IEC 27002:2022	Controalele 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
GDPR	Articolul 32	N/A
Directiva UE NIS2	Articolul 21(2)(d)	N/A
Regulamentul UE DORA	Articolul 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Scop

1.1 Scopul acestei politici este de a defini cerințele organizației pentru protejarea rețelelor interne și externe împotriva accesului neautorizat, indisponibilității serviciilor, interceptării datelor și utilizării abuzive.

1.2 Aceasta asigură protejarea întregii infrastructuri de rețea — inclusiv infrastructura fizică, virtuală, din cloud și din medii hibride — prin controale stratificate, precum segmentarea, aplicarea regulilor de firewall, rutarea securizată și monitorizarea centralizată.

1.3 Această politică impune respectarea clauzei 8.1 din ISO/IEC 27001 și a controalelor din Anexa A 8.20-8.22, asigurând conformitatea cu obligațiile legale și de reglementare aplicabile în temeiul articolului 32 din GDPR, articolului 21 din NIS2 și articolului 9 din DORA.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor rețelelor și componentelor de infrastructură aferente, inclusiv:

2.1.1 routerelor, switch-urilor, punctelor de acces wireless și firewall-urilor

2.1.2 rețelelor virtuale din cloud (de exemplu, AWS VPC, Azure VNet), concentratoarelor VPN și sistemelor SD-WAN

2.1.3 rețelelor LAN interne, zonelor DMZ, căilor de acces la distanță și conexiunilor între sedii sau cu terți

2.1.4 sistemelor-suport, precum DNS, DHCP, servere proxy și echipamente de monitorizare

2.2 Politica este obligatorie pentru întregul personal și pentru furnizorii terți de servicii care gestionează, configurează, monitorizează sau interacționează cu rețelele organizației, fie la sediu, fie în cloud.

2.3 Toate sistemele și aplicațiile conectate la rețelele organizației — indiferent de locație sau de proprietate — trebuie să respecte aceste cerințe de securitate a rețelei.

3. Obiective

3.1 Să asigure confidențialitatea, integritatea și disponibilitatea (CIA) datelor transmise prin rețele, prin controale de acces robuste, rutare securizată și monitorizare.

3.2 Să prevină accesul neautorizat, mișcarea laterală și exploatarea resurselor conectate la rețea prin aplicarea segmentării, zonării și protecției perimetrale.

3.3 Să mențină configurații de rețea consecvente, bazate pe bune practici din industrie și pe informații privind amenințările, pentru a apăra organizația împotriva amenințărilor cibernetice în evoluție.

3.4 Să securizeze comunicațiile externe, interconectivitatea cloud și accesul la distanță prin canale criptate, autentificare strictă și validarea punctelor terminale.

3.5 Să asigure vizibilitatea asupra activității din rețea prin jurnalizare centralizată, inspecția în timp real a traficului și alerte automatizate.

3.6 Să asigure conformitatea cu reglementările prin alinierea tuturor operațiunilor de rețea la cerințele ISO/IEC 27001:2022, GDPR, NIS2, DORA și COBIT 2019.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Deține această politică și se asigură că este revizuită și aliniată la strategia generală de securitate cibernetică a organizației.

4.1.2 Aprobă modelele de segmentare a rețelei, seturile de reguli de firewall pentru sistemele sensibile și solicitările de excepție.

4.2 Managerul de securitate a rețelei / responsabilul cu securitatea infrastructurii

4.2.1 Gestionează arhitectura de apărare a rețelei, inclusiv firewall-urile, sistemele de detectare/prevenire a intruziunilor (IDS/IPS), VPN-urile și rutarea securizată.

4.2.2 Asigură supravegherea segmentării rețelei, a alocărilor VLAN, a zonării traficului și a conectivității externe.

4.2.3 Se asigură de revizuirea continuă a filtrării traficului de intrare și ieșire și de aplicarea modelului Zero Trust la toate nivelurile rețelei.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Cerințe de revizuire și actualizare

9.1 Această politică trebuie revizuită anual de Managerul de securitate a rețelei, în colaborare cu CISO, și actualizată pe baza:

9.1.1 riscurilor emergente (de exemplu, tehnici noi de atac, vulnerabilități de protocol)

9.1.2 schimbărilor de infrastructură (de exemplu, migrări în cloud, implementări SD-WAN)

9.1.3 actualizărilor de reglementare sau de standard care afectează protecția rețelei

9.1.4 constatărilor de audit, tendințelor incidentelor sau degradării performanței cauzate de controale

9.2 Revizuirile trebuie declanșate și de:

9.2.1 schimbări majore ale arhitecturii de rețea

9.2.2 implementarea unor noi platforme de firewall, VPN sau rețea cloud

9.2.3 dezafectarea activelor-cheie sau a zonelor de încredere

9.3 Actualizările trebuie înregistrate în registrul de control al documentelor al SMSI și comunicate către:

9.3.1 echipele de infrastructură și operațiuni de rețea

9.3.2 echipele SOC și de inginerie de securitate

9.3.3 echipele de aplicații care au dependențe de fluxurile de rețea

9.3.4 toți furnizorii terți cu interconectivitate activă

9.4 Toate versiunile anterioare ale politicii trebuie arhivate în condiții de securitate, cu adnotări privind istoricul modificărilor, pentru a păstra caracterul verificabil și trasabilitatea schimbărilor.

10. Politici asociate și interdependențe

10.1 P1 - Politica de securitate a informațiilor. Stabilește principiile fundamentale de securitate și impune protecții stratificate, inclusiv controale de acces și controale de securitate la nivel de rețea.

10.2 P4 - Politica de control al accesului. Asigură aplicarea segmentării rețelei în concordanță cu rolurile utilizatorilor, principiul privilegiului minim și regulile de alocare a accesului.

10.3 P5 - Politica de management al schimbărilor. Reglementează modificările firewall-urilor, ajustările regulilor VPN și schimbările de rutare printr-un proces documentat și verificabil.

10.4 P12 - Politica de management al activelor. Susține identificarea și clasificarea sistemelor conectate la rețea și asigură că toate activele conectate sunt gestionate în cadrul domeniilor de aplicare definite de politici.

10.5 P22 - Politica de jurnalizare și monitorizare. Guvernează colectarea, corelarea și păstrarea jurnalelor de rețea, inclusiv evenimentele firewall, tentativele de acces și detectarea anomaliilor.

10.6 P30 - Politica de răspuns la incidente. Definește procedurile de escaladare, limitare a impactului și eradicare ca răspuns la amenințări sau intruziuni propagate prin rețea, precum DDoS, mișcare laterală sau acces neautorizat.

11. Standarde și cadre de referință

11.1 Această politică este aliniată la standarde internaționale și cerințe de reglementare care definesc operațiuni de rețea securizate, segmentarea, protecția perimetrului și accesul securizat la distanță.

11.2 ISO/IEC 27001

11.2.1 Clauza 8.1 - planificare și control operațional: impune integrarea controalelor tehnice, inclusiv a măsurilor de protecție a rețelei, în procesele operaționale.

11.3 ISO/IEC 27002:2022

11.3.1 Controalele 8.20-8.22: oferă orientări privind protejarea rețelelor, segmentarea serviciilor și securizarea serviciilor de rețea prin controale de acces și monitorizare.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - protecția perimetrului: impune controale de perimetru, segmentare și interconectări securizate.

11.4.2 AC-4 - aplicarea regulilor privind fluxul informațiilor: susține zonarea și restricțiile de trafic bazate pe reguli.

11.4.3 SC-32 - compartimentarea sistemelor informatice: promovează separarea logică a sistemelor informatice.

11.5 GDPR (UE) 2016/679

11.5.1 Articolul 32 - securitatea prelucrării: impune măsuri tehnice — precum firewall-uri și segmentare — pentru protejarea datelor cu caracter personal.

11.6 Directiva UE NIS2 (2022/2555)

11.6.1 Articolul 21(2)(d): impune securitatea eficace a rețelelor și sistemelor informatice, protecția perimetrului, configurarea securizată și controale de separare.

11.7 Regulamentul UE DORA (2022/2554)

11.7.1 Articolul 9 - managementul riscurilor TIC: obligă entitățile financiare să protejeze rețelele și interconectările împotriva accesului neautorizat, scurgerilor de date și perturbărilor operaționale.

11.8 COBIT 2019

11.8.1 DSS01.03 - monitorizarea infrastructurii: impune control proactiv asupra stării și conectivității rețelei.

11.8.2 DSS05.01 - protecție împotriva malware-ului: include segmentarea și controlul perimetrului pentru a reduce propagarea.

11.8.3 MEA03 - monitorizarea, evaluarea și analizarea conformității: consolidează aplicarea politicii de rețea și evaluările de conformitate.