					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P21S					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	-
ISO/IEC 27002:2022	Controlul 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR al UE	Articolul 32	-
Directiva NIS2 a UE	Articolele 21(2)(d), (e)	-
Regulamentul DORA al UE	Articolele 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Scop

1.1. Scopul acestei politici este de a asigura protejarea tuturor comunicațiilor de rețea interne și externe împotriva accesului neautorizat, alterării, interceptării sau utilizării necorespunzătoare, prin controale de securitate clar definite.

1.2. Aceasta stabilește reguli pentru proiectarea, utilizarea și administrarea în condiții de securitate a infrastructurii de rețea, inclusiv a routerelor, punctelor de acces wireless, conexiunilor de acces la distanță și rețelelor segmentate.

1.3. Aceasta urmărește să minimizeze expunerea la amenințări din internet, să asigure confidențialitatea datelor transmise prin rețele interne și externe și să mențină disponibilitatea serviciilor critice.

1.4. Această politică sprijină certificarea ISO/IEC 27001:2022 și contribuie direct la îndeplinirea obligațiilor legale și de reglementare prevăzute de GDPR, NIS2 și DORA, oferind totodată asigurare tehnică clienților și auditorilor.

2. Domeniu de aplicare

2.1. Această politică se aplică tuturor componentelor rețelei IT a organizației, inclusiv:

2.1.1. infrastructurii de rețea cu fir și wireless din locațiile de birou

2.1.2. routerelor, switch-urilor, punctelor de acces, firewall-urilor și gateway-urilor

2.1.3. conexiunilor de acces la distanță, inclusiv VPN, RDP și tunelurilor cloud

2.1.4. aplicațiilor cloud accesate din rețele interne sau externe

2.1.5. dispozitivelor conectate la rețea de către angajați, contractori sau oaspeți

2.2. Această politică reglementează atât segmentele fizice, cât și pe cele logice ale rețelei, inclusiv rețelele pentru oaspeți, dispozitivele din Internetul obiectelor (IoT) și sistemele back-office.

2.3. Politica se aplică întregului personal cu acces la rețeaua organizației, inclusiv:

2.3.1. angajaților interni

2.3.2. lucrătorilor la distanță și personalului în regim hibrid

2.3.3. furnizorilor externi, consultanților și prestatorilor de servicii

2.3.4. oaspeților care utilizează acces Wi-Fi temporar

3. Obiective

3.1. Asigurarea protecției rețelei organizației împotriva accesului neautorizat și a amenințărilor cibernetice externe

3.2. Impunerea unei segmentări adecvate între rețelele de încredere și cele neîncredere (de exemplu, Wi-Fi pentru oaspeți, accesul furnizorilor)

3.3. Asigurarea conectivității securizate la distanță, fără a compromite sistemele interne

3.4. Prevenirea propagării programelor malware și a exfiltrării datelor prin canalele de rețea

3.5. Asigurarea monitorizării, alertării și auditării activității de rețea pentru a sprijini detectarea incidentelor și conformitatea

3.6. Asigurarea faptului că numai dispozitivele aprobate și securizate sunt autorizate să se conecteze la rețelele interne

3.7. Îndeplinirea obligațiilor prevăzute de ISO 27001, GDPR și cadrele relevante de securitate cibernetică

4. Roluri și responsabilități

4.1. Director general (GM)

4.1.1. Este proprietarul acestei politici și asigură alocarea resurselor adecvate pentru proiectarea și administrarea securizată a rețelei.

4.1.2. Revizuiește excepțiile de la controalele de securitate a rețelei și aprobă acordurile de acces la rețea pentru furnizori.

4.1.3. Revizuiește incidentele sau constatările de audit legate de vulnerabilități de securitate la nivelul rețelei.

4.2. Furnizorul de suport IT / rolul IT intern

4.2.1. Implementează, configurează și menține toate firewall-urile, routerele, switch-urile și controlerele wireless.

4.2.2. Gestionează segmentarea dintre rețelele interne, rețelele pentru oaspeți și rețelele externe.

4.2.3. Monitorizează jurnalele și alertele privind tentativele de acces neautorizat sau anomaliile de rețea.

4.2.4. Asigură aplicarea securizată și la timp a actualizărilor de firmware și a modificărilor de configurație.

[... 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. Revizuire anuală

9.1.1. Această politică trebuie revizuită cel puțin o dată pe an de către Directorul general, împreună cu furnizorul de suport IT și coordonatorul de confidențialitate.

9.2. Declanșatori pentru revizuirea intermediară

9.2.1. Revizuirea politicii trebuie declanșată și de:

9.2.1.1. schimbări majore ale arhitecturii de rețea (de exemplu, sisteme VPN sau firewall-uri noi)

9.2.1.2. un incident legat de rețea (de exemplu, intruziune, propagare de ransomware sau exfiltrare de date)

9.2.1.3. actualizări legale, de reglementare sau ale cadrelor aplicabile care afectează protecția rețelei

9.2.1.4. platforme noi ale furnizorilor care necesită metode sau protocoale alternative de acces

9.3. Managementul versiunilor și documentația

9.3.1. Revizuirile politicii trebuie înregistrate cu număr de versiune, dată și rezumat al modificărilor.

9.3.2. Versiunile anterioare trebuie arhivate pentru o perioadă de minimum 3 ani.

9.3.3. Actualizările trebuie comunicate angajaților afectați, cu confirmare obligatorie de luare la cunoștință atunci când sunt introduse schimbări semnificative de comportament.

10. Politici conexe și interdependențe

10.1. Această politică trebuie implementată împreună cu următoarele politici de securitate pentru SME:

10.1.1. P9S – Politica de telemuncă: impune metode securizate de acces la distanță, cerințe privind VPN și protecția terminalelor pentru utilizatorii din afara sediului.

10.1.2. P12S – Politica de management al activelor: asigură că toate sistemele conectate la rețea sunt identificate, clasificate și urmărite împreună cu starea lor actualizată de securitate.

10.1.3. P17S – Politica de protecție a datelor și confidențialitate: asigură că segmentarea rețelei, controalele de acces și jurnalizarea susțin principiile de confidențialitate și protecție a datelor în temeiul GDPR.

10.1.4. P22S – Politica de jurnalizare și monitorizare: specifică cerințele pentru colectarea și revizuirea jurnalelor de la dispozitivele de rețea, conexiunile la distanță și controlerele wireless.

10.1.5. P30S – Politica de răspuns la incidente: definește acțiunile necesare ca răspuns la încălcări ale securității rețelei, tentative de acces neautorizat sau propagarea programelor malware prin rețelele interne.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 8.1 – Impune implementarea controalelor pentru a asigura operațiuni sigure și reziliente, inclusiv la nivelul rețelelor.

11.2. ISO/IEC 27002

11.2.1. Controlul 8.20 – Oferă îndrumări tehnice și procedurale pentru securizarea accesului la rețea, segmentare și monitorizare.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Impune controlul fluxului de informații în cadrul rețelelor și între sisteme.

11.3.2. SC-7 – Impune protecția perimetrului, rutarea securizată și segmentarea rețelei pentru reducerea riscului de acces neautorizat.

11.4. GDPR al UE

11.4.1. Articolul 32 – Impune măsuri tehnice și organizatorice adecvate pentru a asigura confidențialitatea, integritatea și disponibilitatea sistemelor și serviciilor conectate la rețea care prelucrează date cu caracter personal.

11.5. Directiva NIS2 a UE

11.5.1. Articolul 21(2)(d) – Impune măsuri tehnice bazate pe risc, inclusiv securitatea rețelei și controlul accesului.

11.5.2. Articolul 21(2)(e) – Impune segmentarea și izolarea sistemelor pentru a preveni propagarea incidentelor cibernetice.

11.6. DORA a UE

11.6.1. Articolul 9 – Impune organizațiilor implementarea controalelor pentru managementul riscurilor TIC, inclusiv pentru rețele și comunicații securizate.

11.6.2. Articolul 10 – Impune ca strategiile de reziliență digitală să includă protecția infrastructurii de rețea și a conectivității la distanță.

11.7. COBIT 2019

11.7.1. DSS05.02 – Impune protecția eficace a infrastructurii IT și a mediilor de rețea împotriva amenințărilor interne și externe.

11.7.2. APO13.01 – Impune strategii de management al riscurilor care includ segmentarea și monitorizarea rețelei ca parte a atenuării amenințărilor.