					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P02					Titlul documentului: **Politica privind rolurile și responsabilitățile de guvernanță**							
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**

Aliniere la standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 5.3; Anexa A, Controlul 5	
ISO/IEC 27002:2022	Controlul 5	
NIST SP 800-53 Rev. 5	PL-1 până la PL-4, PM-1 până la PM-13	
GDPR	Articolele 5(1)(f), 24, 37	
Directiva UE NIS2	Articolul 21(2)(a)	
Regulamentul UE DORA	Articolul 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Scop

1.1 Această politică definește modelul de guvernanță, rolurile organizaționale și responsabilitățile necesare pentru operarea eficace a unui Sistem de Management al Securității Informației (SMSI).

1.2 Aceasta stabilește linii clare de răspundere, autoritate decizională și trasee de escaladare pentru a asigura integrarea securității informației la toate nivelurile organizației și alinierea acesteia cu obiectivele strategice ale organizației.

1.3 Această politică implementează cerințele clauzei 5.3 și ale controlului A.5.2 din ISO/IEC 27001:2022, asigurând că responsabilitățile pentru activitățile legate de securitate sunt atribuite clar, documentate, comunicate și revizuite periodic.

1.4 Această politică oferă, de asemenea, baza pentru o guvernanță integrată cu alte discipline, precum managementul riscurilor, conformitatea, operațiunile IT și funcțiile juridice.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor persoanelor și entităților implicate în guvernanța, operarea și supravegherea securității informației în cadrul domeniului de aplicare al SMSI. Aceasta include:

2.1.1 conducerea executivă, conducerea de vârf și membrii consiliului de administrație

2.1.2 managerul SMSI, Directorul de Securitate a Informației și proprietarii de control

2.1.3 proprietarii de proces și proprietarii de active

2.1.4 contractorii și furnizorii terți de servicii cu responsabilități de securitate delegate

2.2 Politica acoperă atât funcțiile interne, cât și cele externalizate (de exemplu, un SOC externalizat, administratori ai platformei cloud), în situațiile în care rolurile de guvernanță sunt atribuite formal sau definite contractual.

2.3 Politica se aplică, de asemenea, unităților organizaționale, departamentelor și echipelor de proiect care administrează sau influențează active, sisteme ori servicii relevante pentru securitate.

3. Obiective

3.1 Să asigure că rolurile și responsabilitățile privind securitatea informației sunt definite formal, atribuite, comunicate și documentate.

3.2 Să mențină un model de guvernanță care să impună separarea atribuțiilor, să elimine conflictele de interese și să permită escaladarea problemelor de securitate nerezolvate.

3.3 Să asigure că răspunderea și autoritatea pentru deciziile de securitate sunt distribuite în concordanță cu impactul asupra organizației și cu structura organizațională.

3.4 Să stabilească un cadru pentru gestionarea delegărilor, a schimbărilor de rol și a revizuirii responsabilităților atribuite.

3.5 Să ofere părților interesate — inclusiv autorităților de reglementare, auditorilor și clienților — asigurarea că securitatea informației este guvernată eficace și în conformitate cu standardele aplicabile.

4. Roluri și responsabilități

4.1 managementul executiv (conducerea de vârf)

4.1.1 Asigură supravegherea strategică, alocă resurse și garantează alinierea dintre obiectivele SMSI și obiectivele organizației.

4.1.2 Aprobă documentația majoră a SMSI, inclusiv Politica de securitate a informației, planurile de tratament și deciziile de remediere rezultate din audit.

4.1.3 Participă la revizuirile de management ale SMSI și escaladează pentru aprobare la nivelul consiliului de administrație deciziile care necesită acest nivel de autorizare.

4.1.4 Promovează o cultură a securității și susține respectarea, la nivelul întregii organizații, a principiilor de guvernanță a securității.

4.2 Comitetul de coordonare a securității informației (ISSC)

4.2.1 Acționează ca organism interfuncțional de guvernanță pentru supravegherea SMSI.

4.2.2 Revizuiește profilul de risc, performanța controalelor, constatările de audit și inițiativele strategice de securitate.

4.2.3 Facilitează coordonarea între departamente (de exemplu, IT, Juridic, Resurse Umane, Risc, Conformitate, Operațiuni).

4.2.4 Aprobă pragurile de escaladare, alocările bugetare și modificările de politici care necesită contribuția conducerii executive.

[... 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 Calendar de revizuire

9.1.1 Această politică trebuie revizuită cel puțin anual sau la apariția următoarelor situații:

9.1.1.1 modificări ale structurii organizaționale sau ale echipei executive

9.1.1.2 extinderea sau redefinirea domeniului de aplicare al SMSI

9.1.1.3 modificări de reglementare care afectează atribuirea rolurilor sau supravegherea

9.1.1.4 constatări semnificative de audit sau incidente care implică un eșec de guvernanță

9.2 Procesul de revizuire și aprobare

9.2.1 Managerul SMSI trebuie să inițieze și să conducă procesul de revizuire, inclusiv colectarea contribuțiilor părților interesate și a feedbackului de audit.

9.2.2 Actualizările propuse trebuie revizuite de ISSC și aprobate formal de managementul executiv.

9.2.3 Fiecare versiune trebuie urmărită în Registrul documentelor SMSI și trebuie să includă următoarele metadate:

9.2.3.1 ID-ul și titlul politicii

9.2.3.2 numărul versiunii și rezumatul modificărilor

9.2.3.3 data intrării în vigoare și data următoarei revizuiri

9.2.3.4 proprietarul politicii și aprobatorul

9.2.3.5 nivelul de clasificare al documentului

9.2.3.6 istoricul de păstrare și arhivare

10. Politici conexe și corelări

10.1 Această politică trebuie interpretată împreună cu următoarele politici:

10.1.1 P1 – Politica de securitate a informației: stabilește programul general de securitate și descrie responsabilitățile conducerii privind susținerea politicii și supravegherea strategică.

10.1.2 P5 – Politica de management al schimbărilor: asigură că modificările aduse structurilor de guvernanță, rolurilor sau responsabilităților fac obiectul unei aprobări documentate și al unei revizuiri a riscurilor.

10.1.3 P6 – Politica de management al riscurilor: identifică și tratează riscurile de guvernanță rezultate din conflicte de roluri, atribuții nealocate sau lipsa escaladării.

10.1.4 P7 – Politica de integrare și încetare a raporturilor de muncă: aplică procesele de atribuire și revocare a controalelor pe parcursul schimbărilor din ciclul de viață al personalului.

10.1.5 P33 – Politica de monitorizare a auditului și conformității: sprijină revizuirea independentă a eficacității guvernanței și impune acțiuni corective pentru neconformitate.

10.2 Aceste politici susțin împreună un cadru unificat și aplicabil de guvernanță a SMSI.

11. Standarde și cadre de referință

11.1 Această politică este aliniată cu standarde și cadre recunoscute la nivel global pentru guvernanța securității informației și răspunderea aferentă rolurilor. Aceasta asigură trasabilitatea față de cerințele de reglementare și certificare și susține o structură SMSI robustă și defensabilă.

11.2 ISO/IEC 27001

11.2.1 Clauza 5.3 – Roluri, responsabilități și autorități organizaționale: această politică îndeplinește cerința ca rolurile relevante pentru securitatea informației să fie atribuite clar, comunicate și documentate.

11.2.2 Clauza 9.3 – Revizuirea de management: această politică impune supravegherea executivă a rolurilor și guvernanței SMSI prin revizuiri trimestriale și anuale.

11.2.3 Anexa A, Controlul 5.2 – Roluri și responsabilități privind securitatea informației: definește roluri la nivel tehnic, operațional și strategic pentru a asigura separarea atribuțiilor, asumarea riscurilor și răspunderea trasabilă.

11.3 ISO/IEC 27002:2022 – Controlul 5

11.3.1 Oferă îndrumări de implementare pentru atribuirea responsabilităților privind securitatea informației în cadrul organizației. Această politică adoptă respectivele îndrumări prin definirea tipurilor de roluri, a regulilor de delegare, a procedurilor de escaladare și a mecanismelor de revizuire.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-1 până la PL-4: impun necesitatea unei documentații formale de planificare, inclusiv politici care definesc guvernanța și atribuie responsabilități de securitate.

11.4.2 PM-1 (Planul programului de securitate a informației) și PM-2 (Ofițerul superior pentru securitatea informației): sunt reflectate în această politică prin atribuirea rolului de CISO/Manager SMSI și a rolurilor formale de guvernanță.

11.4.3 PM-5 până la PM-13: această politică îndeplinește cerințele privind documentarea rolurilor, rolurile de risc la nivelul întregii organizații, supravegherea managementului configurației și integrarea cu funcțiile organizației.

11.5 GDPR (UE) 2016/679

11.5.1 Articolul 5(1)(f): impune protejarea datelor cu caracter personal împotriva prelucrării neautorizate sau ilegale. Această politică asigură desemnarea clară și monitorizarea persoanelor responsabile de protecția datelor.

11.5.2 Articolul 24: impune măsuri organizatorice adecvate, inclusiv structuri de guvernanță.

11.5.3 Articolul 37: impune desemnarea unui Responsabil cu Protecția Datelor (DPO), care trebuie reflectată în cadrul de guvernanță al organizației și în registrul responsabilităților.

11.6 Directiva UE NIS2 (2022/2555)

11.6.1 Articolul 21(2)(a): impune entităților implementarea de politici privind analiza riscurilor și securitatea sistemelor informatice, inclusiv responsabilități specifice rolurilor. Această politică definește aceste roluri și mecanismele lor de guvernanță.

11.7 Regulamentul UE DORA (2022/2554)

11.7.1 Articolul 5 – Cadrul de guvernanță și control intern: impune atribuirea formală a responsabilităților pentru managementul riscurilor TIC, a rolurilor decizionale și a canalelor de raportare. Această politică oferă baza pentru guvernanța rolurilor legate de securitate în mediile TIC.

11.8 COBIT 2019

11.8.1 EDM01 – Stabilirea și menținerea cadrului de guvernanță: această politică asigură că SMSI are o structură de guvernanță clar definită, aliniată cu nevoile organizației.

11.8.2 EDM02 – Asigurarea realizării beneficiilor: aliniază activitățile de securitate bazate pe roluri cu obiectivele strategice și operaționale, asigurând răspundere și rezultate măsurabile.

11.8.3 APO01 – Managementul cadrului I&T și APO12 – Managementul riscului: această politică sprijină gestionarea structurată a rolurilor privind securitatea informației în cadrul mai larg de guvernanță IT și management al riscului.

11.8.4 MEA01 – Monitorizare, evaluare și analiză a performanței: integrează mecanisme de revizuire pentru a verifica dacă rolurile de guvernanță sunt eficace, actuale și aplicate.