					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P02S					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	
ISO/IEC 27002:2022	Controale: 5.2, 5.3, 5	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
GDPR al UE	Articolele 5(2), 32	

1. Scop

1.1 Prezenta politică stabilește modul în care responsabilitățile de guvernanță pentru securitatea informației sunt alocate, delegate și gestionate în cadrul organizației, pentru a asigura conformitatea deplină cu ISO/IEC 27001:2022 și cu alte obligații de reglementare aplicabile.

1.2 Aceasta asigură responsabilitatea la toate nivelurile și sprijină eficacitatea operațională prin identificarea clară a persoanelor responsabile pentru fiecare funcție legată de securitate.

1.3 Prezenta politică consolidează capacitatea organizației de a demonstra conformitatea în cadrul auditurilor și crește încrederea clienților prin demonstrarea unei guvernanțe formale a securității, inclusiv în organizațiile cu personal tehnic limitat sau cu servicii IT externalizate.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor persoanelor care gestionează sisteme sau date ale organizației, inclusiv:

2.1.1 proprietarilor de procese de business, Directorului general

2.1.2 angajaților și contractorilor

2.1.3 furnizorilor externi de servicii IT sau consultanților

2.2 Aceasta acoperă toate sistemele, mediile și serviciile utilizate pentru prelucrarea, transmiterea sau stocarea informațiilor de business sau ale clienților, inclusiv:

2.2.1 infrastructura IT de birou și dispozitivele utilizate pentru telemuncă

2.2.2 platformele cloud și serviciile de poștă electronică

2.2.3 înregistrările fizice și unitățile partajate

2.3 Domeniul de aplicare include atât activitățile interne, cât și cele externalizate care implică guvernanța securității informației.

3. Obiective

3.1 Stabilirea unei responsabilități clare pentru toate atribuțiile legate de securitate, inclusiv managementul politicilor, controlul accesului, gestionarea incidentelor și monitorizarea.

3.2 Asigurarea unei separări eficace a atribuțiilor pentru a reduce conflictele de interese sau riscurile de fraudă.

3.3 Asigurarea documentării clare a sarcinilor și rolurilor de securitate, precum și a revizuirii periodice a acestora.

3.4 Asigurarea unui proces decizional informat, a escaladării și a supravegherii riscurilor IT și de securitate.

3.5 Sprijinirea certificării ISO/IEC 27001:2022 și consolidarea încrederii clienților, partenerilor și auditorilor.

4. Roluri și responsabilități

4.1 Director general / Proprietar de proces de business

4.1.1 Poartă responsabilitatea deplină pentru implementarea și supravegherea prezentei politici.

4.1.2 Aprobă toate rolurile de securitate, responsabilitățile și deciziile de delegare.

4.1.3 Monitorizează conformitatea și ia deciziile finale privind excepțiile de la politică și escaladările.

4.2 Coordonator de securitate desemnat (dacă este numit)

4.2.1 Poate fi un membru al personalului sau un consultant de încredere.

4.2.2 Acest rol poate fi îndeplinit de Directorul general sau de un furnizor extern în mediile de microîntreprindere.

4.2.3 Oferă sprijin pentru aplicarea curentă a controlului accesului, răspunsului la incidente sau a activităților tehnice de bază în materie de securitate.

4.2.4 Raportează direct Directorului general orice problemă sau risc de securitate.

[... 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 Prezenta politică trebuie revizuită de Directorul general la fiecare 12 luni pentru a se asigura că reflectă în continuare obligațiile legale, nevoile operaționale și cerințele de certificare ISO/IEC 27001.

9.2 Revizuiri intermediare

9.2.1 Revizuirile trebuie efectuate și atunci când:

9.2.1.1 au loc schimbări organizaționale majore

9.2.1.2 este integrat un nou furnizor

9.2.1.3 are loc un incident grav de securitate

9.2.1.4 reglementări precum GDPR, NIS2 sau DORA sunt actualizate

9.3 Controlul versiunilor și documentarea

9.3.1 Toate revizuirile trebuie să includă:

9.3.1.1 data revizuirii

9.3.1.2 rezumatul modificărilor

9.3.1.3 semnătura Directorului general sau o aprobare documentată a acestuia

9.3.1.4 versiunile anterioare arhivate pentru referință în audit

9.4 Comunicarea modificărilor

9.4.1 Toate actualizările politicii trebuie comunicate prompt personalului și furnizorilor prin e-mail, portaluri interne sau note formale.

10. Politici conexe și corelări

10.1 Prezenta politică trebuie implementată împreună cu următoarele politici SME, pentru asigurarea eficacității:

10.1.1 P4S – Politica de control al accesului: definește modul în care accesul este acordat, gestionat și retras, în corelare directă cu rolurile alocate și supravegherea.

10.1.2 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: consolidează responsabilitățile și așteptările specifice rolurilor.

10.1.3 P17S – Politica privind protecția datelor și confidențialitatea: stabilește obligațiile legale prevăzute de GDPR, care sunt alocate rolurilor definite în această politică de guvernanță.

10.1.4 P30S – Politica de răspuns la incidente: impune responsabilități definite pentru raportarea, escaladarea și soluționarea incidentelor.

10.2 Împreună, aceste politici asigură aplicare consecventă, responsabilitate internă și conformitate externă.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 5.3 – Roluri, responsabilități și autorități organizaționale: impune ca rolurile să fie alocate clar și susținute de conducerea de vârf.

11.2 ISO/IEC 27002

11.2.1 Controalele 5.2–5.4: impun documentarea clară a rolurilor privind securitatea informației, separarea atribuțiilor și supravegherea managerială.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: stabilește un program general de securitate a informației cu responsabilități definite.

11.3.2 PL-1 până la PL-4: impun controale de planificare, inclusiv elaborarea politicilor și atribuirea documentată a rolurilor.

11.3.3 CA-1: impune roluri definite pentru evaluare și autorizare.

11.3.4 AC-1: corelează controalele de acces bazate pe roluri cu responsabilitățile de guvernanță alocate.

11.4 GDPR al UE

11.4.1 Articolul 5(2) – Responsabilitate: impune organizațiilor să demonstreze conformitatea prin roluri și responsabilități.

11.4.2 Articolul 32 – Securitatea prelucrării: subliniază alocarea clară a atribuțiilor pentru protejarea datelor cu caracter personal.

11.5 NIS a UE

11.5.1 Articolul 21(2)(a): impune structuri de guvernanță care includ roluri formalizate pentru gestionarea riscului cibernetic și a incidentelor.

11.6 DORA a UE

11.6.1 Articolele 9 și 10: impun entităților financiare să aloce și să supravegheze clar responsabilitățile legate de TIC și de securitate.

11.7 COBIT 2019

11.7.1 EDM03 – Asigurarea optimizării riscului: impune roluri bine definite și trasee de escaladare pentru gestionarea riscurilor de securitate.

11.7.2 APO13 – Gestionarea securității: alocă persoanelor și rolurilor atribuții strategice și operaționale de securitate.

11.7.3 DSS05 – Gestionarea serviciilor de securitate: impune structură și trasabilitate în responsabilitățile aferente serviciilor de securitate externe și interne.