					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P06S					Titlul documentului: **Politica de management al riscurilor**							
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	Clauzele 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 până la RA-7, PM-9	
Directiva NIS2 a UE	Articolul 21(2)(a–d)	
Regulamentul DORA al UE	Articolul 5	
COBIT 2019	APO12, MEA01	

1. Scop

1.1 Această politică definește modul în care organizația identifică, evaluează și gestionează riscurile legate de securitatea informațiilor, operațiuni, tehnologie și servicii prestate de terți.

1.2 Aceasta asigură că procesul de management al riscurilor este o componentă activă a planificării, execuției proiectelor, selecției furnizorilor și răspunsului la incidente, în conformitate cu ISO 27001, ISO 31000 și cerințele de reglementare.

1.3 Politica sprijină procesul decizional bazat pe risc, protecția activelor informaționale și reziliența activităților operaționale esențiale ale organizației.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 Tuturor departamentelor, sistemelor și utilizatorilor din cadrul organizației

2.1.2 Tuturor informațiilor, serviciilor și activelor gestionate intern sau prin intermediul terților

2.1.3 Activităților legate de risc, inclusiv revizuirilor de proiect, actualizărilor majore de sistem, externalizării și conformității cu reglementările

2.2 Aceasta include toate tipurile de riscuri, cum ar fi:

2.2.1 Amenințări de securitate cibernetică și vulnerabilități ale sistemelor

2.2.2 Perturbări operaționale și indisponibilități ale serviciilor

2.2.3 Expuneri juridice, de conformitate sau reputaționale

2.2.4 Riscuri asociate terților și lanțului de aprovizionare

2.3 Toți angajații, contractanții și furnizorii de servicii trebuie să respecte această politică atunci când identifică sau raportează riscuri.

3. Obiective

3.1 Integrarea unor proceduri simple și repetabile de evaluare a riscurilor în activitățile operaționale curente ale organizației.

3.2 Identificarea și prioritizarea riscurilor care ar putea afecta confidențialitatea, integritatea, disponibilitatea (CIA) sau conformitatea juridică.

3.3 Atribuirea responsabilității și definirea acțiunilor de tratare a riscurilor pentru toate riscurile semnificative.

3.4 Menținerea unui Registru al riscurilor corect și actualizat pentru a susține demonstrarea conformității și urmărirea stării riscurilor.

3.5 Asigurarea implicării conducerii în aprobarea toleranței la risc și a planurilor majore de tratament.

4. Roluri și responsabilități

4.1 Director general

4.1.1 Stabilește apetitul la risc al organizației și aprobă cadrul de management al riscurilor.

4.1.2 Aprobă deciziile majore privind tratamentul riscului și resursele aferente.

4.1.3 Revizuiește trimestrial principalele riscuri împreună cu coordonatorul de risc.

4.2 Coordonator de risc (sau responsabilul SMSI)

4.2.1 Facilitează evaluările de risc și menține Registrul riscurilor.

4.2.2 Se asigură că evaluarea riscurilor, alocarea responsabilității pentru risc și activitățile de tratare a riscurilor sunt documentate.

4.2.3 Organizează cel puțin o revizuire formală a riscurilor pe an.

[... 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 Revizuirea anuală a politicii

9.1.1 Această politică trebuie revizuită cel puțin o dată pe an de către Directorul general și coordonatorul de risc pentru a asigura relevanța și caracterul complet.

9.2 Declanșatori pentru actualizare

9.2.1 Revizuirea și actualizarea anticipată trebuie efectuate dacă:

9.2.1.1 Un incident major sau o constatare de audit evidențiază lacune în gestionarea riscurilor

9.2.1.2 Sunt introduse noi unități operaționale, tehnologii sau parteneriate

9.2.1.3 Se modifică o cerință de reglementare sau contractuală

9.3 Controlul versiunilor

9.3.1 Toate actualizările acestei politici trebuie gestionate prin controlul versiunilor, cu următoarele metadate:

9.3.1.1 Numărul versiunii și data intrării în vigoare

9.3.1.2 Rezumatul modificărilor

9.3.1.3 Aprobatorul (Director general)

9.3.1.4 Versiunile anterioare arhivate în scopuri de audit

9.4 Comunicare și conștientizare

9.4.1 Versiunile actualizate ale politicii și planurile majore de tratament al riscului trebuie comunicate personalului vizat. Instruirea anuală de reîmprospătare trebuie să includă principiile de bază privind conștientizarea riscurilor.

10. Politici conexe și corelări

10.1 Această politică funcționează în coordonare cu alte politici pentru a asigura o guvernanță cuprinzătoare a securității:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: definește cine răspunde pentru deținerea riscului și pentru luarea deciziilor.

10.1.2 P5S – Politica de management al schimbărilor: impune evaluarea riscurilor înainte de implementarea schimbărilor tehnice sau de proces.

10.1.3 P17S – Politica privind protecția datelor și confidențialitatea: abordează riscul de reglementare asociat gestionării datelor cu caracter personal.

10.1.4 P30S – Politica de răspuns la incidente: asigură continuitatea tratamentului riscului în timpul și după incidentele de securitate.

10.1.5 P33S – Politica de continuitate a activității: identifică riscurile reziduale și măsurile de recuperare pentru serviciile critice.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:

11.1.1 Clauza 6.1 – stabilește un proces formal de management al riscurilor și de planificare a tratamentului.

11.1.2 Clauza 6.1.3 – impune organizațiilor să păstreze planuri de tratament și aprobări documentate.

11.2 ISO/IEC 27002:

11.2.1 Controalele 5.4, 5.25 – oferă orientări de implementare pentru alocarea responsabilității privind riscul, prioritizare și managementul ciclului de viață.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 până la RA-7 – definesc evaluarea riscurilor, strategiile de răspuns, documentarea și mecanismele de revizuire.

11.4 PM-9 – impune o supraveghere consecventă, la nivel managerial, a riscurilor organizației.

11.5 Directiva NIS2 a UE

11.5.1 Articolul 21(2)(a–d) – impune controale obligatorii de evaluare a riscurilor, atenuare și guvernanță pentru entitățile esențiale și importante.

11.6 Regulamentul DORA al UE

11.6.1 Articolul 5 – impune entităților reglementate să definească și să gestioneze cadre de management al riscurilor TIC, inclusiv identificarea, clasificarea și răspunsul.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: integrează riscul în planificarea strategică și operațională.

11.7.2 MEA01 – Monitor, Evaluate, and Assess: asigură eficacitatea și conformitatea proceselor și acțiunilor privind riscul.