					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P06					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, 8.32, 10	Fundamentul identificării și managementului riscurilor, integrarea în managementul schimbărilor, îmbunătățire continuă
ISO/IEC 27005:2024	Metodologie pentru întregul ciclu de viață al riscului	Proces complet de management al riscurilor, în conformitate cu standardul
ISO 31000:2018	Principii și cadru de management al riscurilor	Principii de management al riscurilor adoptate în cadrul organizației
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Ghid și structură pentru evaluări de risc, guvernanță multistratificată a riscurilor
RGPD al UE	Articolele 24, 25, 32	Procese și controale privind riscurile aferente protecției datelor
Directiva NIS2 a UE	Articolul 21(2)(a–d)	Obligații privind evaluarea riscurilor și securitatea
Regulamentul DORA al UE	Articolele 5, 6	Managementul riscurilor TIC și reziliență operațională
COBIT 2019	APO12, MEA	Structura și supravegherea managementului riscurilor

1. Scop

1.1 Prezenta politică stabilește un cadru unitar și formalizat pentru identificarea, analiza, evaluarea, tratarea, monitorizarea și revizuirea riscurilor de securitate a informației la nivelul întregii organizații.

1.2 Aceasta asigură aplicarea consecventă a principiilor bazate pe risc, care protejează confidențialitatea, integritatea și disponibilitatea (CIA) activelor informaționale, în conformitate cu clauza 6.1 din ISO/IEC 27001:2022 și ISO 31000:2018.

1.3 Politica integrează managementul riscurilor de securitate a informației în procesele decizionale ale organizației pentru îndeplinirea obiectivelor strategice interne și a cerințelor externe de reglementare.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor unităților organizaționale, proceselor de afaceri, sistemelor, personalului și relațiilor cu terți implicați în manipularea, dezvoltarea, stocarea sau gestionarea activelor informaționale.

2.2 Domeniul de aplicare se extinde asupra activelor fizice, digitale și găzduite în cloud, inclusiv date structurate și nestructurate, aplicații, infrastructură, rețele și servicii.

2.3 Aceasta acoperă riscurile de securitate a informației la nivel strategic, operațional, de proiect și tehnic și este obligatorie pentru toți angajații, contractanții și furnizorii de servicii implicați în activități ale Sistemului de management al securității informației (SMSI).

2.4 Managementul riscurilor trebuie aplicat în următoarele scenarii:

2.4.1 implementarea unui proiect nou sau a unui sistem nou

2.4.1.1 schimbări semnificative (de exemplu, arhitectură, proprietate, procese)

2.4.1.2 integrarea furnizorilor și acorduri cu terți

2.4.1.3 răspuns la incidente și revizuiri post-incident

2.4.1.4 revizuiri periodice ale riscurilor la nivel organizațional sau audituri

3. Obiective

3.1 Stabilirea și operaționalizarea unui proces repetabil de management al riscurilor la nivelul întregii organizații, bazat pe metodologiile ISO/IEC 27005 și ISO 31000.

3.2 Asigurarea faptului că riscurile sunt identificate, analizate, evaluate și tratate prin metode structurate și cu trasabilitate, inclusiv prin alocarea responsabilității pentru risc și corelarea cu controalele.

3.3 Menținerea unui Registru al riscurilor și a unui Plan de tratare a riscurilor, centralizate și supuse controlului versiunilor, care să reflecte statutul curent al riscurilor, acoperirea controalelor și progresul măsurilor de atenuare.

3.4 Alinierea deciziilor privind riscurile cu apetitul la risc documentat și cu nivelurile de toleranță definite și facilitarea adoptării unor decizii de guvernanță informate privind acceptarea, atenuarea, transferul sau evitarea riscurilor.

3.5 Monitorizarea continuă a tendințelor de risc și asigurarea eficacității tratamentelor aplicate, precum și posibilitatea unor ajustări proactive pe baza evoluției amenințărilor sau a schimbărilor din activitățile organizației.

4. Roluri și responsabilități

4.1 Conducerea executivă / Consiliul de administrație

4.1.1 Aprobă cadrul de management al riscurilor și definește apetitul la risc acceptabil și pragurile de toleranță.

4.1.2 Autorizează strategiile de tratare a riscurilor pentru riscurile reziduale care depășesc toleranța.

4.1.3 Alocă resurse și asigură supravegherea necesară pentru funcționarea eficace a programului de management al riscurilor.

4.2 Managerul SMSI / Responsabilul cu riscurile

4.2.1 Este proprietarul prezentei politici și asigură alinierea acesteia cu standardele ISO/IEC 27001 și 27005.

4.2.2 Coordonează procesul de evaluare a riscurilor la nivelul organizației și menține Registrul riscurilor și Planul de tratare a riscurilor.

4.2.3 Asigură revizuiri periodice și escaladarea riscurilor-cheie către conducerea executivă sau Comitetul de coordonare al SMSI.

[... 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 Prezenta politică și cadrul asociat trebuie revizuite anual sau:

9.1.1 după un eveniment major de risc sau un incident de securitate

9.1.2 în urma unei schimbări organizaționale sau tehnice semnificative

9.1.3 ca răspuns la constatări de audit sau la noi cerințe de reglementare

9.2 Managerul SMSI, Responsabilul cu riscurile și echipa de conformitate sunt responsabili în comun pentru:

9.2.1 inițierea ciclului de revizuire

9.2.2 colectarea contribuțiilor din partea unităților de business

9.2.3 revizuirea procedurilor și a pragurilor, după caz

9.3 Toate reviziile trebuie să fie:

9.3.1 supuse controlului versiunilor și înregistrate

9.3.2 aprobate de conducerea executivă

9.3.3 comunicate părților interesate

9.3.4 păstrate în depozitul de audit pentru o perioadă minimă de 5 ani

10. Politici conexe și corelări

10.1 Prezenta politică este interdependentă cu următoarele politici de securitate a informației:

10.1.1 P1 – Politica de securitate a informației: stabilește modelul general de guvernanță a securității în baza căruia funcționează această politică de risc.

10.1.2 P2 – Politica privind rolurile și responsabilitățile de guvernanță: definește deținătorii responsabilităților și nivelurile de guvernanță menționate în matricea de escaladare a riscurilor.

10.1.3 P5 – Politica de management al schimbărilor: declanșează reevaluarea riscurilor pentru schimbări de infrastructură și organizaționale.

10.1.4 P13 – Politica de clasificare și etichetare a datelor: sprijină evaluarea impactului în timpul identificării riscurilor.

10.1.5 P33 – Politica de monitorizare a auditului și conformității: validează respectarea politicii, inclusiv caracterul complet al Registrului riscurilor și dovezile tratamentelor.

11. Standarde și cadre de referință

11.1 Prezenta politică este aliniată în mod explicit cu următoarele standarde și cadre, pentru a asigura respectarea celor mai bune practici internaționale și a așteptărilor de reglementare privind managementul riscurilor de securitate a informației:

11.2 ISO/IEC 27001:

11.2.1 Clauza 6.1: stabilește cerințele pentru identificarea riscurilor și oportunităților, inclusiv ciclul complet de viață al evaluărilor și tratamentelor riscurilor de securitate a informației. Prezenta politică operaționalizează clauzele 6.1 și 6.1.2 printr-un cadru structurat care impune protocoale documentate pentru identificarea, analiza, evaluarea, tratarea riscurilor și acceptarea riscului rezidual.

11.2.2 Clauza 8.32: integrarea gândirii bazate pe risc în procesele de management al schimbărilor asigură că toate schimbările organizaționale semnificative declanșează reevaluări formale ale riscurilor.

11.2.3 Clauza 10: îmbunătățirea continuă este integrată prin revizuiri regulate ale politicii, analiza tendințelor de risc și actualizări ale SoA determinate de informațiile rezultate din analiza riscurilor.

11.3 ISO/IEC 27005:

11.3.1 Oferă orientări specializate și detaliate privind managementul riscurilor de securitate a informației. Prezenta politică implementează întregul model de proces al ISO/IEC 27005: stabilirea contextului, identificarea riscurilor, analiza riscului, evaluarea riscurilor, tratarea riscului, acceptarea riscului, comunicarea riscurilor, monitorizarea și revizuirea riscurilor.

11.4 ISO 31000:

11.4.1 Prezenta politică integrează principiile ISO 31000, precum angajamentul conducerii, integrarea în procesul decizional și îmbunătățirea continuă. Aceasta asigură integrarea managementului riscurilor în cultura și operațiunile organizației.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Este aliniată cu ghidul NIST pentru efectuarea evaluărilor de risc, inclusiv identificarea amenințărilor, analiza vulnerabilităților, estimarea probabilității și determinarea impactului. Structura

prezentei politici reflectă etapele de evaluare a riscului definite de NIST și le adaptează atât pentru procese tehnice, cât și pentru procese de afaceri.

11.6 NIST SP 800-39:

11.6.1 Sprijină guvernanța riscurilor la nivel organizațional, punând accent pe managementul riscurilor pe niveluri: organizațional, misiune/proces de afaceri și sistem informatic. Politica asigură definirea clară a responsabilității pentru risc la toate nivelurile și include strategii de tratare la nivel organizațional.

11.7 RGPD al UE:

11.7.1 Articolul 24: impune implementarea unor măsuri tehnice și organizatorice adecvate pentru a asigura gestionarea corespunzătoare a riscurilor privind protecția datelor — aspect tratat prin procesul structurat de risc prevăzut în această politică.

11.7.2 Articolul 25: „protecția datelor începând cu momentul conceperii și în mod implicit" este aliniată cu integrarea tratamentului riscurilor în proiectarea sistemelor și a proceselor.

11.7.3 Articolul 32: impune o abordare bazată pe risc a măsurilor de securitate — îndeplinită prin evaluări de risc bazate pe impact și selectarea controalelor pe baza riscului.

11.8 Directiva NIS2 a UE:

11.8.1 Articolul 21(2)(a–d): impune entităților să efectueze evaluări de risc, să implementeze politici privind analiza riscurilor și să asigure măsuri de securitate proporționale. Prezenta politică îndeplinește aceste obligații prin aplicarea continuă a ciclului de viață al riscurilor și prin guvernanță documentată.

11.9 Regulamentul DORA al UE:

11.9.1 Articolul 5: impune un cadru documentat de management al riscurilor TIC — acoperit integral prin arhitectura acestei politici, inclusiv corelarea cu SoA și indicatorii-cheie de risc.

11.9.2 Articolul 6: impune integrarea managementului riscurilor în strategiile de reziliență operațională, aspect tratat prin matrici de escaladare și urmărirea activelor critice.

11.10 COBIT 2019:

11.10.1 APO12 – Manage Risk: se corelează direct cu instituirea de către organizație a unei abordări structurate de management al riscurilor, prin alocarea rolurilor, urmărirea tratamentelor și asigurarea responsabilității la nivelul consiliului.

11.10.2 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: este reflectat în accentul pus de această politică pe analiza tendințelor, monitorizarea indicatorilor-cheie de risc și integrarea feedbackului din audit în ciclurile de îmbunătățire continuă.