					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P33S					Titlul documentului: **Politica de audit și monitorizare a conformității**							
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	Clauzele 9.2, 10	Audituri interne, îmbunătățire continuă și remedierea neconformităților
ISO/IEC 27002:2022	Controalele 5.35, 5.37	Revizuiri interne planificate, revizuiri independente pentru procese externalizate
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Evaluări de securitate, monitorizare continuă, revizuirea/analiza/raportarea auditului
GDPR al UE	Articolele 24 și 32	Auditarea măsurilor tehnice și organizatorice, dovezi privind eficacitatea controalelor
Directiva NIS2 a UE	Articolul 21(2)(f)	Revizuire proactivă și conformitate bazată pe dovezi
Regulamentul DORA al UE	Articolul 10	Managementul riscurilor TIC, monitorizare și raportare
COBIT 2019	MEA01, MEA03	Monitorizarea/evaluarea conformității, conformitate, pregătire pentru revizuiri efectuate de terți

1. Scop

1.1 Prezenta politică stabilește abordarea organizației privind desfășurarea auditurilor interne, verificarea controalelor de securitate și monitorizarea conformității cu cerințele de reglementare. Aceasta asigură faptul că toate controalele, politicile, sistemele și furnizorii de servicii sunt supuși unor revizuiri regulate și structurate.

1.2 Scopul este identificarea deficiențelor de control, prevenirea neconformității și demonstrarea diligenței necesare în raport cu ISO/IEC 27001, GDPR și cadrele conexe.

1.3 Aceasta permite IMM-urilor să mențină controlul operațional și pregătirea pentru certificare, chiar și în absența unui departament dedicat de conformitate, prin utilizarea unor liste de verificare simple, repetabile și a unor constatări prioritizate în funcție de risc.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică următoarelor:

2.1.1 tuturor departamentelor interne și furnizorilor externi de servicii cu responsabilități legate de sistemele IT, datele cu caracter personal și serviciile critice pentru activitățile organizației

2.1.2 tuturor controalelor și sistemelor aflate în domeniul de aplicare al Sistemului de management al securității informației (SMSI)

2.1.3 tuturor auditurilor interne, revizuirilor controalelor de securitate și verificărilor de conformitate, indiferent dacă sunt efectuate intern sau de un consultant extern, client sau autoritate de reglementare

2.2 Prezenta politică se aplică, de asemenea, colectării de dovezi și raportării pentru:

2.2.1 audituri de certificare și recertificare ISO/IEC 27001

2.2.2 audituri de protecție a datelor desfășurate în temeiul GDPR sau al cerințelor contractuale

2.2.3 chestionare de securitate inițiate de clienți sau evaluări de tip due diligence

2.2.4 orice revizuiri de reglementare sau independente în temeiul NIS2 sau DORA, după caz

3. Obiective

3.1 Asigurarea faptului că toate controalele și politicile-cheie sunt revizuite periodic din perspectiva eficacității și conformității.

3.2 Menținerea pistei de audit și a înregistrărilor privind acțiunile corective pentru a demonstra asumarea responsabilității și îmbunătățirea continuă.

3.3 Pregătirea pentru certificare, recertificare și programe de asigurare solicitate de clienți (de exemplu, ISO 27001, integrarea furnizorilor).

3.4 Identificarea timpurie a lacunelor, pentru a permite remedierea promptă înainte ca problemele să escaladeze sau să conducă la încălcarea obligațiilor.

3.5 Sprijinirea Directorului general și a Furnizorului de suport IT în coordonarea revizuirilor cu un nivel minim de complexitate, asigurând în același timp rezultate solide și susținute de dovezi.

4. Roluri și responsabilități

4.1 Director general (GM)

4.1.1 Asigură supravegherea programului de audit

4.1.2 Aprobă planurile de revizuire internă și constatările

4.1.3 Alocă și monitorizează acțiunile corective

4.1.4 Autorizează implicarea auditorilor sau consultanților externi

4.2 Furnizor de suport IT / administrator

4.2.1 Furnizează dovezi în cadrul auditurilor interne și externe (de exemplu, jurnale, configurații, înregistrări privind controlul accesului)

4.2.2 Acordă sprijin pentru verificările tehnice (de exemplu, starea copiilor de siguranță, conformitatea aplicării patch-urilor)

4.2.3 Menține depozitul de dovezi de audit

[... 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 și a planului de audit

9.1.1 Directorul general (GM) trebuie să revizuiască prezenta politică și calendarul de audit cel puțin o dată pe an.

9.1.2 Revizuirea trebuie să evalueze:

9.1.2.1 eficacitatea auditurilor în identificarea lacunelor

9.1.2.2 rata de finalizare a auditurilor și a acțiunilor corective

9.1.2.3 modificările cerințelor legale, de reglementare sau de certificare aplicabile

9.2 Actualizări declanșate de evenimente

9.2.1 Politica trebuie revizuită și actualizată atunci când:

9.2.2 un audit de certificare sau de supraveghere conduce la o neconformitate majoră

9.2.3 cadrele juridice sau de reglementare se modifică (de exemplu, noi orientări GDPR, transpunerea națională a NIS2)

9.2.4 schimbările din organizație afectează sistemele, procesele sau furnizorii incluși în domeniul de aplicare al auditului

9.2.5 un incident critic sau o încălcare a securității relevă lacune de control nedetectate anterior

9.3 Documentarea actualizărilor

9.3.1 Toate reviziile trebuie urmărite într-un jurnal de control al versiunilor politicii

9.3.2 Actualizările trebuie distribuite tuturor membrilor echipei implicați în audituri

9.3.3 Un rezumat al modificărilor trebuie inclus împreună cu politica actualizată pentru a asigura înțelegerea acesteia

10. Politici conexe și interdependențe

10.1 Prezenta politică este susținută de și consolidează mai multe alte politici SME:

10.1.1 P1S – Politica de securitate a informației: stabilește baza de referință pentru toate cerințele privind controalele și impune respectarea acestora prin audituri.

10.1.2 P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește responsabilitatea pentru planificarea auditului, execuția acestuia și asumarea acțiunilor corective.

10.1.3 P6S – Politica de management al riscurilor: identifică punctele slabe ale controalelor evidențiate în audituri și asigură documentarea constatărilor în Registrul riscurilor.

10.1.4 P17S – Politica de protecție a datelor și confidențialitate: definește controalele GDPR care trebuie auditate, inclusiv gestionarea datelor, răspunsul la încălcări și notele de informare privind confidențialitatea.

10.1.5 P22S – Politica de jurnalizare și monitorizare: furnizează jurnalele de audit și datele criminalistice utilizate în cadrul revizuirilor de conformitate și al controalelor.

10.1.6 P30S – Politica de răspuns la incidente: impune auditarea periodică a înregistrărilor incidentelor și a revizuirilor post-eveniment pentru verificarea eficacității răspunsului.

10.1.7 P31S – Politica privind colectarea dovezilor și criminalistica digitală: furnizează procedurile pentru colectarea de dovezi verificabile, cu lanț de custodie, în timpul auditurilor.

10.2 Împreună, aceste politici creează un cadru de control cu buclă închisă, care permite verificarea internă, asigurarea externă și guvernanța aliniată la standarde.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001:

11.1.1 Clauza 9.2 – impune audituri interne pentru evaluarea performanței SMSI și a alinierii la cerințe.

11.1.2 Clauza 10.1 – impune îmbunătățirea continuă pe baza rezultatelor auditului și a remedierii neconformităților.

11.2 ISO/IEC 27002:

11.2.1 Controlul 5.35 – impune revizuiri interne planificate ale controalelor și proceselor.

11.2.2 Controlul 5.37 – subliniază necesitatea unor revizuiri independente, în special pentru procesele externalizate.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Evaluări de securitate: impune auditarea controalelor implementate pentru verificarea eficacității.

11.3.2 CA-7 – Monitorizare continuă: subliniază detectarea proactivă și revizuirea deficiențelor controalelor.

11.3.3 AU-6 – Revizuirea, analiza și raportarea auditului: impune analiza periodică și soluționarea jurnalelor de audit și a constatărilor.

11.4 GDPR al UE:

11.4.1 Articolele 24 și 32 – impun implementarea și auditarea măsurilor tehnice și organizatorice, inclusiv dovezi privind eficacitatea controalelor și îmbunătățirea în timp.

11.5 Directiva NIS2 a UE (2022/2555):

11.5.1 Articolele 20–21 – impun revizuirea proactivă a controalelor, conformitatea bazată pe dovezi și caracterul auditabil pentru entitățile esențiale și importante.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: impune evaluarea periodică a performanței proceselor și controalelor în raport cu standardele și obiectivele.

11.6.2 MEA03 – Ensure Compliance with External Requirements: se concentrează pe monitorizarea internă și pregătirea pentru audituri efectuate de terți și revizuiri de reglementare.