					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P01S					Titlul documentului: **Politica de securitate a informației**							
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 5.1, 5.2, 5.3, 6.1, 6.2, 8	Specifică angajamentul conducerii, cerințele privind politica, atribuirea rolurilor, evaluarea riscurilor și controlul operațional
ISO/IEC 27002:2022	Controalele 5.1–5	Specifică elaborarea politicilor documentate de securitate a informației, atribuirea rolurilor, separarea atribuțiilor și responsabilitățile managementului
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Cerințe privind planul programului de securitate, politica de planificare, evaluarea/autorizarea și controlul accesului
GDPR al UE (2016/679)	Articolul 5(2), Articolul 32	Principiul responsabilității și măsuri privind securitatea prelucrării, în special pentru rolurile documentate
Directiva NIS2 a UE (2022/2555)	Articolul 21(2)(a)	Impune măsuri de management al riscurilor, precum și roluri și responsabilități pentru riscul cibernetic
Regulamentul DORA al UE (2022/2554)	Articolul 9, Articolul 10	Impune atribuirea rolurilor pentru managementul riscurilor TIC și continuitatea activității
COBIT 2019	EDM03, APO13, DSS05	Asigură optimizarea riscurilor, managementul securității și managementul serviciilor de securitate prin atribuirea clară a rolurilor

1. Scop

1.1 Prezenta politică demonstrează angajamentul organizației noastre de a proteja informațiile clienților și informațiile organizației prin definirea clară a responsabilităților și a măsurilor practice de securitate, adecvate organizațiilor fără echipe IT dedicate.

1.2 Aceasta asigură că toți angajații, contractanții și furnizorii de servicii respectă reguli obligatorii, permițând conformitatea deplină cu cerințele de certificare ISO/IEC 27001.

1.3 Prezenta politică permite organizației noastre să consolideze încrederea clienților prin demonstrarea clară a modului în care le protejăm informațiile, prin responsabilități definite, procese structurate și responsabilitate clară.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor persoanelor care accesează sau gestionează datele și sistemele organizației, inclusiv:

2.1.1 Proprietarilor afacerii și directorilor generali

2.1.2 Angajaților, contractanților, stagiarilor

2.1.3 Furnizorilor externi de servicii IT sau consultanților

2.2 Aceasta acoperă toate tipurile de informații, sisteme și servicii, inclusiv:

2.2.1 Evidențe de afaceri, date ale clienților, parole și e-mailuri

2.2.2 Echipamente IT hardware, precum laptopuri și telefoane

2.2.3 Servicii cloud utilizate pentru stocarea fișierelor, comunicare sau activități financiare

2.2.4 Documente fizice păstrate în spațiile de birouri

2.3 Politica se aplică în toate mediile de lucru — la birou, la distanță și în medii cloud — și include toate dispozitivele și aplicațiile software utilizate pentru prelucrarea sau stocarea informațiilor organizației.

3. Obiective

3.1 Atribuirea clară a responsabilității: securitatea informației trebuie să aibă întotdeauna un responsabil. De regulă, acesta este Directorul general sau persoana desemnată formal de acesta.

3.2 Protejarea informațiilor clienților și ale organizației: trebuie implementate măsuri de protecție fiabile și consecvente pentru a preveni utilizarea necorespunzătoare, pierderea sau furtul datelor sensibile, inclusiv evidențele clienților și evidențele financiare.

3.3 Sprijinirea certificării ISO/IEC 27001: politica trebuie să permită organizației să demonstreze conformitatea deplină cu cerințele ISO/IEC 27001, asigurând pregătirea pentru audit și eligibilitatea pentru certificare fără a necesita o infrastructură complexă.

3.4 Integrarea securității în activitățile operaționale ale organizației: securitatea informației trebuie integrată în activitățile și deciziile zilnice din întreaga organizație.

3.5 Dezvoltarea conștientizării și a culturii de securitate: fiecare angajat trebuie să înțeleagă și să respecte practicile de securitate, cum ar fi utilizarea unor parole puternice și raportarea activităților suspecte.

4. Roluri și responsabilități

4.1 Director general sau proprietar al afacerii

4.1.1 Deține responsabilitatea deplină pentru securitatea informației.

4.1.2 Aprobă și menține prezenta politică.

4.1.3 Se asigură că toate activitățile esențiale de securitate sunt gestionate direct sau delegate în scris.

4.1.4 Verifică faptul că toate activitățile de securitate delegate (cum ar fi managementul accesului sau răspunsul la incidente) sunt îndeplinite în mod eficace.

4.1.5 Acționează ca punct de contact implicit pentru toate aspectele de securitate interne și externe, inclusiv pentru audituri și solicitările clienților.

4.1.6 Monitorizează progresul în raport cu aceste obiective în cadrul revizuirii anuale. Obiectivele trebuie să fie măsurabile, acolo unde este posibil (de exemplu, procentul personalului instruit, numărul incidentelor raportate etc.), și revizuite pe baza constatărilor de securitate și a modificărilor profilului de risc.

4.2 Angajat desemnat (dacă este cazul)

4.2.1 Poate sprijini Directorul general prin gestionarea activităților curente, precum crearea conturilor de utilizator, retragerea accesului pentru persoanele care părăsesc organizația sau coordonarea cu furnizorul IT.

4.2.2 Trebuie să fie desemnat oficial și să dispună de suficientă autoritate și de instrumentele necesare pentru îndeplinirea activităților.

4.2.3 Raportează orice problemă Directorului general.

[... 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 (DG) cel puțin o dată pe an pentru a asigura conformitatea continuă cu cerințele de certificare ISO/IEC 27001, modificările de reglementare (cum ar fi GDPR, NIS2 și DORA) și evoluția nevoilor organizației.

9.2 Revizuiri intermediare

9.2.1 Revizuiri suplimentare trebuie efectuate ori de câte ori apar schimbări semnificative, cum ar fi:

9.2.1.1 Incidente majore de securitate sau încălcări ale securității.

9.2.1.2 Introducerea unor noi procese sau tehnologii ale organizației (de exemplu, software nou, platforme de lucru la distanță sau servicii cloud).

9.2.1.3 Modificări ale cerințelor legale sau de reglementare care afectează gestionarea informațiilor.

9.3 Documentarea modificărilor

9.3.1 Toate revizuirile și modificările politicii trebuie documentate formal, menționând clar data, natura revizuirilor și aprobarea DG.

9.3.2 Un istoric al versiunilor politicii trebuie menținut în condiții de securitate pentru a demonstra evoluția politicii și conformitatea în timpul auditurilor.

9.4 Comunicarea actualizărilor

9.4.1 Orice modificare a prezentei politici trebuie comunicată prompt tuturor angajaților, contractanților și terților relevanți.

9.4.2 Versiunile actualizate ale politicii trebuie să fie ușor accesibile întregului personal afectat (de exemplu, distribuite electronic sau afișate fizic la locul de muncă).

10. Politici conexe și corelări

10.1 Prezenta politică interacționează îndeaproape cu alte politici din setul de politici SME al organizației, în special:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: clarifică atribuirea sarcinilor și responsabilităților de securitate.

10.1.2 P4S – Politica de control al accesului: definește gestionarea securizată a accesului la informațiile companiei.

10.1.3 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: furnizează îndrumări esențiale pentru instruirea și conștientizarea personalului.

10.1.4 P17S – Politica privind protecția datelor și confidențialitatea: asigură conformitatea cu GDPR și alte legi privind protecția datelor.

10.1.5 P30S – Politica de răspuns la incidente: descrie în detaliu acțiunile necesare ca răspuns la incidente de securitate.

10.2 Aceste politici conexe oferă îndrumare operațională clară și trebuie implementate împreună pentru a asigura conformitatea deplină cu cerințele de certificare ISO/IEC 27001.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 5.1 – Leadership și angajament: impune angajamentul conducerii de vârf și responsabilitatea pentru eficacitatea securității informației în cadrul organizației.

11.1.2 Clauza 5.2 – Politica de securitate a informației: impune politici clare și documentate, aliniate la strategia organizației și la cerințele de conformitate.

11.1.3 Clauza 5.3 – Roluri și responsabilități organizaționale: definește atribuirea clară a responsabilităților privind securitatea informației în întreaga organizație, esențială pentru o guvernanță eficace și pentru conformitatea în audit.

11.1.4 Clauza 6.1 – Acțiuni pentru tratarea riscurilor și oportunităților: asigură că riscurile privind securitatea informației sunt identificate, evaluate și tratate în mod sistematic.

11.1.5 Clauza 8.1 – Planificare și control operațional: impune organizației să planifice și să implementeze procesele necesare pentru îndeplinirea obiectivelor de securitate a informației și pentru gestionarea eficace a riscurilor asociate.

11.2 ISO/IEC 27002:2022 Controalele 5.1–5

11.2.1 Anexa A Controlul 5.1 – Politici pentru securitatea informației: specifică elaborarea și comunicarea politicilor documentate de securitate a informației.

11.2.2 Anexa A Controlul 5.2 – Roluri de securitate a informației: clarifică și atribuie formal rolurile și responsabilitățile privind securitatea informației părților relevante.

11.2.3 Anexa A Controlul 5.3 – Separarea atribuțiilor: impune separarea clară a atribuțiilor pentru a reduce conflictele de interese și riscurile de fraudă în gestionarea informațiilor sensibile.

11.2.4 Anexa A Controlul 5.4 – Responsabilitățile managementului: impune ca managementul să demonstreze angajament față de securitatea informației prin supraveghere activă și alocare de resurse.

11.2.5 Consolidează necesitatea unor politici, roluri, responsabilități și structuri de guvernanță privind securitatea informației clar documentate, asigurând un management consecvent și trasabilitate pentru audit la nivelul întregii organizații.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Planul programului de securitate a informației: impune strategii și politici documentate de guvernanță a securității informației, oferind un cadru pentru implementare și management consecvent.

11.3.2 PL-1 – Politica de planificare a securității: impune o politică de planificare a securității la nivelul întregii organizații pentru a ghida operarea securizată și alinierea strategică a activităților de securitate a informației.

11.3.3 CA-1 – Politica de evaluare și autorizare a securității: impune roluri clar definite pentru evaluare și autorizare, pentru a asigura eficacitatea continuă și conformitatea cu cerințele de securitate a informației.

11.3.4 AC-1 – Politica de control al accesului: impune organizațiilor să definească, să documenteze și să aplice în mod clar practicile și responsabilitățile de management al accesului.

11.4 GDPR al UE (2016/679)

11.4.1 Articolul 5(2) – Principiul responsabilității: impune organizațiilor să demonstreze conformitatea cu principiile protecției datelor, inclusiv prin roluri și politici documentate pentru responsabilitățile privind protecția datelor.

11.4.2 Articolul 32 – Securitatea prelucrării: impune implementarea de măsuri tehnice și organizatorice adecvate, inclusiv responsabilități clare de securitate, pentru a proteja datele cu caracter personal împotriva încălcărilor și a accesului neautorizat.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(a) – Măsuri de management al riscurilor: impune mecanisme clare de guvernanță, inclusiv roluri și responsabilități definite pentru securitatea informației, esențiale pentru gestionarea eficace a riscurilor cibernetice.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 9 – Managementul riscurilor TIC: impune organizațiilor să atribuie clar rolurile și responsabilitățile legate de managementul riscurilor TIC, consolidând reziliența și pregătirea pentru continuitatea activității.

11.6.2 Articolul 10 – Continuitatea activităților TIC: impune responsabilitate clară și roluri structurate pentru menținerea rezilienței și continuității TIC, asigurând că organizațiile pot răspunde în mod fiabil la perturbări.

11.7 COBIT 2019

11.7.1 EDM03 – Asigurarea optimizării riscurilor: subliniază responsabilitatea și rolurile clar definite în gestionarea riscurilor organizației, oferind o guvernanță solidă și o supraveghere eficace a riscurilor de securitate a informației.

11.7.2 APO13 – Managementul securității: impune organizațiilor să stabilească și să comunice clar responsabilitățile de management al securității, asigurând alinierea la obiectivele organizației și la cerințele de reglementare.

11.7.3 DSS05 – Managementul serviciilor de securitate: solicită roluri structurate și responsabilități clare în gestionarea serviciilor de securitate, permițând implementarea consecventă și verificarea conformității.