					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P01					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**

Notă juridică (drepturi de autor și restricții de utilizare)

(C) 2025 Clarysec LLC. All rights reserved.

Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.

Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.

Pentru licențiere, contactați: info@clarysec.com

1. Scop

1.1 Prezenta politică definește angajamentul general al organizației față de securitatea informației prin instituirea unui Sistem de management al securității informației (SMSI) formal.

1.2 Aceasta stabilește direcția strategică și cerințele fundamentale pentru protejarea confidențialității, integrității, disponibilității și rezilienței tuturor activelor informaționale din mediile fizice, digitale și cloud.

1.3 Politica îndeplinește cerințele clauzelor 5.1 și 5.2 din ISO/IEC 27001:2022 prin exprimarea intenției conducerii, a angajamentului conducerii de vârf și a alinierii activităților de securitate la obiectivele organizației.

1.4 Aceasta constituie referința autorizată pentru toate politicile subordonate, standardele și procedurile din cadrul SMSI și este esențială pentru susținerea unui mediu de securitate bazat pe risc, orientat către conformitate și supus îmbunătățirii continue.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor persoanelor, activelor și proceselor definite în domeniul de aplicare al SMSI, inclusiv:

2.1.1 tuturor unităților de afaceri, departamentelor, filialelor și sucursalelor;

2.1.2 angajaților, contractanților, personalului temporar, consultanților și furnizorilor terți de servicii;

2.1.3 tuturor datelor, sistemelor informatice, aplicațiilor, infrastructurii și canalelor de comunicații;

2.1.4 tuturor mediilor fizice, cloud, la distanță și hibride în care datele companiei sunt prelucrate sau accesate.

2.2 Politica este obligatorie pentru toate entitățile care gestionează informațiile organizației și se aplică tuturor etapelor din ciclul de viață al informației, de la creare și transmitere până la stocare și eliminare.

2.3 Orice excluderi sau limitări din acest domeniu de aplicare trebuie documentate în declarația privind domeniul de aplicare al SMSI și justificate prin aprobare formală din partea conducerii executive.

3. Obiective

3.1 Instituirea unui SMSI conform cu ISO/IEC 27001:2022 și capabil să susțină un proces decizional bazat pe risc la nivelul întregii organizații.

3.2 Asigurarea integrării principiilor de confidențialitate, integritate și disponibilitate în toate activitățile, sistemele și parteneriatele organizației.

3.3 Asigurarea conformității cu cerințele de reglementare și contractuale prin definirea unor obiective de securitate măsurabile, stabilite prin politici, și prin integrarea acestora în activitățile operaționale ale organizației.

3.4 Reducerea probabilității și a impactului incidentelor de securitate a informației prin controale preventive, detective și corective eficace.

3.5 Susținerea îmbunătățirii continue a maturității securității informației prin indicatori de performanță definiți, rezultate ale auditului și analize efectuate de management.

3.6 Promovarea unei culturi a responsabilității, conștientizării și rezilienței, în care responsabilitățile de securitate sunt înțelese și îndeplinite de întregul personal.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Aprobă și susține politica de securitate a informației și cadrul SMSI.

4.1.2 Asigură alinierea dintre obiectivele de securitate și strategia de afaceri.

4.1.3 Oferă exemplu personal și promovează o cultură solidă a securității informației.

4.1.4 Revizuiește și aprobă modificările majore ale domeniului de aplicare al SMSI, ale tratamentului riscului și ale structurii de guvernanță.

4.2 Directorul pentru securitatea informației (CISO) / Managerul SMSI

4.2.1 Deține responsabilitatea pentru SMSI și menține această politică în conformitate cu ISO/IEC 27001.

4.2.2 Coordonează procesele de evaluare a riscurilor, implementare a controalelor și îmbunătățire continuă.

4.2.3 Asigură coordonarea interfuncțională a eforturilor de securitate și supraveghează politicile subordonate.

4.2.4 Raportează conducerii executive stadiul SMSI, incidentele, rezultatele auditului și indicatorii.

4.2.5 Asigură efectuarea revizuirilor și actualizărilor politicii în conformitate cu secțiunea 9 din prezentul document.

[... 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 Frecvența revizuirii

9.1.1 Prezenta politică trebuie revizuită cel puțin anual sau la apariția oricăruia dintre următorii factori declanșatori:

9.1.1.1 schimbări semnificative ale obligațiilor legale, de reglementare sau contractuale;

9.1.1.2 modificări semnificative ale profilului de risc al organizației;

9.1.1.3 rezultate ale auditurilor interne sau externe;

9.1.1.4 incidente majore sau deficiențe majore ale controalelor.

9.2 Autoritatea și procesul de revizuire

9.2.1 CISO sau Managerul SMSI desemnat trebuie să coordoneze procesul de revizuire.

9.2.2 Elementele de intrare pentru revizuire trebuie să includă:

9.2.2.1 rezultatele auditului intern;

9.2.2.2 tendințe rezultate din evaluările de risc;

9.2.2.3 schimbări ale proceselor organizației și ale tehnologiei;

9.2.2.4 performanța în raport cu indicatorii-cheie de performanță și pragurile de risc.

9.2.3 Toate actualizările trebuie:

9.2.3.1 să fie gestionate prin controlul versiunilor și documentate;

9.2.3.2 să fie aprobate de managementul executiv;

9.2.3.3 să fie distribuite tuturor părților afectate prin canalele oficiale de comunicare;

9.2.3.4 să declanșeze actualizările necesare ale documentației subordonate și ale instruirii.

10. Politici conexe și corelări

10.1 Această politică fundamentală este corelată direct cu următoarele politici și cadre de securitate ale organizației:

10.1.1 P2 – Politica privind rolurile și responsabilitățile de guvernanță: definește structura de guvernanță și ierarhia autorității la care se face referire în acest document.

10.1.2 P3 – Politica de utilizare acceptabilă: stabilește cerințele comportamentale și utilizarea adecvată a activelor informaționale.

10.1.3 P4 – Politica de control al accesului: transpune în practică controalele de acces derivate din această politică-cadru.

10.1.4 P6 – Politica de management al riscurilor: furnizează contextul bazat pe risc pentru selectarea controalelor și acceptarea riscurilor reziduale.

10.1.5 P33 – Politica de audit și monitorizare a conformității: descrie modul în care mecanismele interne de asigurare validează aplicarea politicii.

10.2 Aceste interdependențe asigură alinierea completă și trasabilitatea la nivelul SMSI și susțin o guvernanță unitară a riscurilor și a conformității.

11. Standarde și cadre de referință

11.1 Această politică de securitate a informației este aliniată formal cu următoarele standarde și cadre pentru a asigura conformitatea deplină, pregătirea pentru audit și susținerea în raport cu cerințele de reglementare:

11.2 ISO/IEC 27001

11.2.1 Clauza 5.1 – Leadership și angajament: această politică demonstrează angajamentul conducerii de vârf față de securitatea informației și definește responsabilitățile și alocările de resurse pentru SMSI.

11.2.2 Clauza 5.2 – Politica de securitate a informației: acest document servește drept politica formală de securitate a organizației, aliniată cu obiectivele de securitate declarate, strategia de afaceri și cerințele ISO/IEC 27001.

11.2.3 Clauza 6.1 – Acțiuni pentru tratarea riscurilor și oportunităților: abordarea bazată pe risc reflectată în această politică asigură aplicarea proporțională a resurselor de securitate în raport cu amenințările.

11.2.4 Clauza 9.2 – Audit intern și Clauza 10 – Îmbunătățire: această politică este integrată în ciclul de îmbunătățire continuă al organizației și face obiectul validării prin audit intern.

11.2.5 ISO/IEC 27002:2022 – Controlul 5.1: specifică îndrumări pentru instituirea și menținerea politicilor de securitate. Această politică reflectă recomandările ISO/IEC 27002 privind documentația ierarhică, ciclurile de revizuire și aplicabilitatea.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Politica și procedurile de planificare a securității): această politică îndeplinește cerința de a elabora, comunica și revizui o politică formală de securitate a informației la nivelul întregii organizații.

11.3.2 PM-1 până la PM-5: abordează guvernanța la nivel de program, inclusiv rolurile de securitate a informației, alocarea resurselor, strategia de risc și integrarea planificării securității în operațiunile organizației.

11.4 GDPR UE (2016/679)

11.4.1 Articolul 5(2): impune principiul responsabilității. Această politică definește părțile responsabile și acțiuni de aplicare trasabile.

11.4.2 Articolul 24: impune implementarea de măsuri tehnice și organizatorice, inclusiv politici aliniate la risc.

11.4.3 Articolul 32: susține implementarea de măsuri adecvate pentru asigurarea securității datelor cu caracter personal pe întreg ciclul lor de viață.

11.5 Directiva UE NIS2 (2022/2555)

11.5.1 Articolul 21(2)(a): obligă entitățile să implementeze o politică de securitate documentată care abordează managementul riscurilor și guvernanța. Această politică îndeplinește această cerință și susține, în sens mai larg, pregătirea în materie de securitate cibernetică și protecția infrastructurilor critice.

11.6 Regulamentul UE DORA (2022/2554)

11.6.1 Articolul 5(2): impune un cadru de control intern documentat pentru managementul riscurilor TIC. Această politică susține conformitatea în sectorul financiar prin alocarea de roluri, controale și funcții de supraveghere aliniate așteptărilor de guvernanță prevăzute de DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Stabilirea cadrului de guvernanță: această politică susține guvernanța corporativă prin definirea rolurilor SMSI, a angajamentelor conducerii și a obiectivelor strategice.

11.7.2 APO01 – Cadru de management: susține instituirea și operarea unui SMSI structurat.

11.7.3 APO12 – Managementul riscurilor: furnizează baza pentru guvernanța riscurilor de securitate a informației.

11.7.4 MEA01/MEA03 – Monitorizare, evaluare și analiză: consolidează evaluarea continuă a performanței și monitorizarea controlului intern prin aplicarea conformității cu politica.