					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P26					Titlul documentului: **Politica de securitate privind terții și furnizorii**							
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	Clauza 8	Planificare și control operațional: impune controale formale asupra serviciilor furnizate de terți care au impact asupra Sistemului de management al securității informației (SMSI)
ISO/IEC 27002:2022	Controalele 5.19–5.22	Politici și proceduri pentru relațiile cu furnizorii; managementul riscului asociat furnizorilor; managementul furnizării serviciilor de către furnizori; monitorizarea și revizuirea furnizorilor
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Servicii de sisteme externe; managementul configurației pentru dezvoltatori; interconectări de sisteme; securitatea personalului terților
GDPR	Articolele 28, 32, 33	Obligațiile persoanei împuternicite; securitatea prelucrării; notificarea unei încălcări a securității datelor cu caracter personal
Directiva UE NIS2	Articolul 21(2)(e–f)	managementul furnizorilor bazat pe risc și supravegherea securității
Regulamentul UE DORA	Articolele 28, 30	riscul TIC asociat terților, supravegherea furnizorilor terți critici de servicii TIC
COBIT 2019	BAI05, DSS02, MEA03	Gestionarea facilitării schimbării organizaționale; gestionarea cererilor de servicii și a incidentelor; monitorizarea, evaluarea și analizarea conformității

1. Scop

1.1 Prezenta politică definește cerințele de securitate a informației pentru stabilirea, gestionarea și menținerea unor relații securizate cu terți și furnizori de servicii.

1.2 Aceasta asigură că toți furnizorii care au acces la datele, sistemele sau infrastructura organizației fac obiectul unor controale de securitate riguroase, al unor garanții contractuale și al unei supravegheri continue pe întreg ciclul de viață al serviciului.

1.3 Politica sprijină controalele 5.19–5.22 din Anexa A la ISO/IEC 27001 prin integrarea cerințelor de securitate în achiziții, integrarea furnizorilor, diligența necesară, managementul contractelor, monitorizarea serviciilor și procesele de încetare.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 tuturor furnizorilor terți, contractorilor, furnizorilor de servicii cloud și organizațiilor de servicii care prelucrează sau accesează active informaționale ale organizației;

2.1.2 tuturor rolurilor interne implicate în evaluarea furnizorilor, integrarea furnizorilor, contractare, managementul riscurilor, monitorizare sau încetare;

2.1.3 tuturor relațiilor cu furnizorii care includ acces la date sensibile, integrare cu servicii de producție sau suport pentru funcții critice ale organizației.

2.2 Politica acoperă atât furnizorii direcți, cât și subcontractanții acestora, după caz, și include software furnizat de terți, infrastructură, suport și servicii administrate.

3. Obiective

3.1 Să asigure că riscurile de securitate asociate furnizorilor sunt identificate, evaluate și tratate în mod consecvent pe întreg ciclul de viață al relației.

3.2 Să integreze cerințe de securitate standardizate în toate contractele cu furnizorii, inclusiv obligații privind notificarea încălcărilor, clauze privind dreptul de audit și responsabilități privind protecția datelor.

3.3 Să impună diligență necesară formală și evaluări de risc documentate înainte de angajarea unor furnizori noi sau de reînnoirea acordurilor de servicii cu risc ridicat.

3.4 Să stabilească mecanisme pentru monitorizarea continuă a conformității furnizorilor, inclusiv revizuiri de performanță, audituri și escaladarea incidentelor.

3.5 Să gestioneze modificările aduse serviciilor furnizorilor și să impună încetarea colaborării în condiții de securitate, precum și returnarea/distrugerea datelor la încetarea relației contractuale.

3.6 Să alinieze controalele de securitate aplicabile terților la obligațiile de reglementare și contractuale aplicabile, inclusiv GDPR, NIS2, DORA și standardele ISO/IEC 27001.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Deține această politică și asigură alinierea acesteia cu Sistemul de management al securității informației (SMSI), managementul riscurilor și strategia de conformitate.

4.1.2 Aprobă nivelurile de clasificare a furnizorilor, rezultatele revizuirilor de securitate și excepțiile cu risc ridicat.

4.1.3 Participă la escaladarea incidentelor grave asociate furnizorilor și la negocierile contractuale pentru servicii critice.

4.2 Achiziții și managementul furnizorilor

4.2.1 Asigură că toate contractele noi și reînnoite cu furnizorii includ clauze aprobate privind securitatea și protecția datelor.

4.2.2 Menține registrul centralizat al furnizorilor și se coordonează cu funcțiile juridice și de conformitate pentru documentarea riscurilor asociate terților.

4.2.3 Inițiază procesele de integrare a furnizorilor și asigură alinierea cu evaluările de securitate efectuate înainte de contractare.

[... 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 Această politică trebuie revizuită cel puțin anual sau mai devreme în cazul:

9.1.1 unor schimbări semnificative ale strategiei de achiziții sau ale ecosistemului de furnizori;

9.1.2 actualizării cadrului juridic sau de reglementare (de exemplu, DORA, GDPR);

9.1.3 unor incidente majore asociate terților, încălcări ale securității datelor sau neconformități rezultate din audit;

9.1.4 unor constatări rezultate din evaluări de risc sau din partea organismelor externe de certificare.

9.2 Procesul de revizuire este deținut în comun de CISO, achiziții, funcția juridică și funcțiile de management al riscurilor.

9.3 Toate revizuirile politicii trebuie documentate în registrul de control al documentelor al SMSI, supuse controlului versiunilor și comunicate părților interesate relevante prin canalele de guvernanță a furnizorilor și prin programe de conștientizare pentru angajați.

9.4 Versiunile înlocuite trebuie arhivate pentru o perioadă minimă de trei ani, pentru trasabilitate și conformitate juridică.

10. Politici conexe și interdependențe

10.1 P1 – Politica de securitate a informației. Stabilește angajamentul general de a securiza toate activitățile organizației, inclusiv cele bazate pe furnizori terți și furnizori externi de servicii.

10.2 P6 – Politica de management al riscurilor. Ghidează identificarea, evaluarea și tratarea riscurilor asociate relațiilor cu terți, inclusiv riscurile moștenite sau sistemice din ecosistemele furnizorilor.

10.3 P17 – Politica de protecție a datelor și confidențialitate. Se aplică tuturor furnizorilor care gestionează date cu caracter personal și impune termeni contractuali adecvați, măsuri de protecție pentru transferuri și principiile protecției datelor încă din faza de proiectare.

10.4 P4 – Politica de control al accesului. Reglementează modul în care personalul terților obține acces la sistemele organizației, impunând permisiuni bazate pe roluri, controale ale sesiunilor și proceduri de revocare.

10.5 P22 – Politica de jurnalizare și monitorizare. Impune ca accesul furnizorilor la sisteme să fie monitorizat, jurnalizat și revizuit, în special în mediile în care au loc activități privilegiate sau activități centrate pe date.

10.6 P30 – Politica de răspuns la incidente. Definește procedurile de escaladare și cerințele de raportare a încălcărilor pentru evenimente de securitate generate de furnizori sau pentru investigații comune care implică sisteme ale terților.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001: Clauza 8.1 – Planificare și control operațional: impune controale formale asupra serviciilor furnizate de terți care au impact asupra SMSI.

11.2 ISO/IEC 27002:2022 – Controalele 5.19–5.22:

11.2.1 Controlul 5.19 din Anexa A – Politici și proceduri pentru relațiile cu furnizorii: impune controale pentru gestionarea interacțiunilor cu furnizorii.

11.2.2 Controlul 5.20 din Anexa A – Managementul riscului asociat furnizorilor: se concentrează pe identificarea, evaluarea și supravegherea continuă a profilului de risc al securității furnizorilor.

11.2.3 Controlul 5.21 din Anexa A – Managementul furnizării serviciilor de către furnizori: impune alinierea performanței și a securității la așteptările contractuale.

11.2.4 Controlul 5.22 din Anexa A – Monitorizarea și revizuirea furnizorilor: consolidează necesitatea validării și reevaluării continue a conformității terților.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Servicii de sisteme externe: definește cerințele de securitate și de risc pentru sistemele operate de entități externe.

11.3.2 SA-10 – Managementul configurației pentru dezvoltatori: se aplică atunci când terții livrează software sau medii.

11.3.3 CA-3 – Interconectări de sisteme: impune supravegherea și stabilirea de acorduri privind fluxurile de date între entități.

11.3.4 PS-7 – Securitatea personalului terților: asigură că personalul contractorilor și al furnizorilor este verificat și monitorizat în mod adecvat.

11.4 GDPR (UE) 2016/679:

11.4.1 Articolul 28 – Obligațiile persoanei împuternicite: impune acorduri scrise cu persoanele împuternicite care să includă măsuri tehnice și organizatorice (TOMs).

11.4.2 Articolul 32 – Securitatea prelucrării: impune măsuri de protecție adecvate atât pentru operatori, cât și pentru persoanele împuternicite.

11.4.3 Articolul 33 – Notificarea unei încălcări a securității datelor cu caracter personal: impune notificarea promptă din partea furnizorilor în caz de încălcare.

11.5 Directiva UE NIS2 (2022/2555):

11.5.1 Articolul 21(2)(e–f): impune managementul furnizorilor bazat pe risc și supravegherea securității, în special în lanțurile de aprovizionare digitale ale entităților esențiale și importante.

11.6 Regulamentul UE DORA (2022/2554):

11.6.1 Articolul 28 – Riscul TIC asociat terților: impune obligații privind evaluarea riscurilor, termeni contractuali de securitate și strategii de ieșire pentru furnizorii de servicii financiare.

11.6.2 Articolul 30 – Supravegherea furnizorilor terți critici de servicii TIC: stabilește cerințe sporite de monitorizare și supraveghere pentru furnizorii-cheie.

11.7 COBIT 2019:

11.7.1 BAI05 – Gestionarea facilitării schimbării organizaționale: asigură guvernanța securizată a tranzițiilor asociate furnizorilor.

11.7.2 DSS02 – Gestionarea cererilor de servicii și a incidentelor: se aplică problemelor raportate de furnizori și integrării gestionării incidentelor.

11.7.3 MEA03 – Monitorizarea, evaluarea și analizarea conformității: consolidează măsurarea performanței furnizorilor și monitorizarea conformității.