					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P26S					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	Controale operaționale pentru relațiile cu terții și furnizorii
ISO/IEC 27002:2022	Controalele 5.19–5.22	Controale de securitate pentru furnizori, clauze contractuale de securitate, managementul schimbărilor, monitorizare și revizuire
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Achiziția, configurarea, acordurile de interconectare și controalele privind personalul extern
RGPD al UE	Articolele 28, 32	Acorduri de prelucrare a datelor, cerințe de securitate pentru persoanele împuternicite
Directiva NIS2 a UE	Articolele 21(2)(a)(b)(i), 23(1)	managementul riscurilor din lanțul de aprovizionare, supravegherea serviciilor prestate de terți
Regulamentul DORA al UE	Articolele 5(1)(2), 28(1)(2)	Managementul riscurilor TIC pentru furnizorii terți de servicii
COBIT 2019	APO10, APO12, DSS05	managementul furnizorilor și integrarea riscurilor

1. Scop

1.1 Prezenta politică stabilește cerințele obligatorii de securitate pentru inițierea, gestionarea și încetarea relațiilor cu terți și furnizori care accesează sau influențează datele, sistemele sau serviciile organizației.

1.2 Aceasta asigură că furnizorii externi — inclusiv furnizorul de suport IT, furnizorii de servicii cloud, dezvoltatorii de software și contractanții pentru procese operaționale — gestionează în mod securizat activele companiei, în conformitate cu legislația și standardele aplicabile.

1.3 Prezenta politică reduce riscuri precum scurgerile de date, modificările neautorizate în sisteme, sancțiunile de reglementare sau întreruperile activităților organizației cauzate de relații cu terți nesecurizate sau guvernate necorespunzător.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor terților care:

2.1.1 Furnizează software, infrastructură, servicii de găzduire sau servicii cloud

2.1.2 Accesează sau administrează sisteme, dispozitive sau aplicații interne

2.1.3 Gestionează date, documente sau copii de siguranță ale companiei

2.1.4 Susțin activitățile operaționale ale organizației, resursele umane, funcția financiară sau serviciile pentru clienți

2.2 De asemenea, se aplică:

2.2.1 Personalului intern implicat în selecția, contractarea sau supravegherea furnizorilor

2.2.2 Oricărui membru al personalului care gestionează integrarea furnizorilor, contractele, accesul sau revizuirile

2.2.3 Oricărui sistem sau proces care depinde de componente sau servicii furnizate de terți

3. Obiective

3.1 Să se asigure că toți furnizorii îndeplinesc cerințe de securitate clar definite.

3.2 Să se impună includerea în contractele cu furnizorii a unor obligații aplicabile privind securitatea, confidențialitatea și răspunsul la incidente.

3.3 Să se evalueze și să se documenteze riscurile asociate furnizorilor înainte de semnarea acordurilor sau de acordarea accesului.

3.4 Să se efectueze revizuiri periodice ale furnizorilor cu risc ridicat sau ale furnizorilor critici pentru confirmarea conformității.

3.5 Să se stabilească un proces formal pentru excepții, managementul incidentelor și actualizarea contractelor.

3.6 Să se susțină conformitatea cu obligațiile prevăzute de ISO/IEC 27001:2022, RGPD, NIS2 și DORA referitoare la guvernanța furnizorilor.

4. Roluri și responsabilități

4.1 Director general (GM)

4.1.1 Are responsabilitatea finală pentru selecția furnizorilor și conformitatea în materie de securitate

4.1.2 Aprobă contractele, excepțiile și escaladările care implică furnizori

4.1.3 Asigură supravegherea răspunsului la incidente și a procesului decizional atunci când furnizorii nu își îndeplinesc obligațiile

4.2 Furnizorul IT sau persoana internă de contact pentru securitate

4.2.1 Evaluează accesul tehnic solicitat de furnizori

4.2.2 Implementează reguli de control al accesului, revizuiește jurnalele și verifică gestionarea securizată a datelor

4.2.3 Revizuiește dovezile privind controalele de securitate, certificările sau rezultatele auditurilor, după caz

[... 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 trebuie revizuită cel puțin anual de Directorul general, cu participarea furnizorului IT sau a responsabilului cu managementul furnizorilor.

9.2 Politica trebuie, de asemenea, revizuită:

9.2.1 După orice schimbare semnificativă a obligațiilor legale, de reglementare sau contractuale

9.2.2 În urma unui incident de securitate asociat unui furnizor sau a unei constatări de audit

9.2.3 La introducerea unor noi categorii de furnizori (de exemplu, platforme SaaS critice)

9.3 Toate actualizările trebuie să fie:

9.3.1 Documentate, cu istoric al versiunilor și justificare

9.3.2 Aprobate de Directorul general

9.3.3 Comunicate personalului intern relevant și responsabililor cu managementul furnizorilor

9.3.4 Păstrate împreună cu versiunile anterioare, conform P14S – Politica de păstrare și eliminare a datelor

10. Politici asociate și interdependențe

10.1 Eficacitatea prezentei politici depinde de coordonarea cu următoarele politici SME privind securitatea informației:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: atribuie responsabilitatea pentru supravegherea furnizorilor și aplicarea obligațiilor contractuale.

10.1.2 P4S – Politica de control al accesului: stabilește regulile de restricționare a accesului care trebuie aplicate atunci când furnizorilor li se acordă acces la sisteme.

10.1.3 P17S – Politica de protecție a datelor și confidențialitate: asigură că furnizorii care prelucrează date cu caracter personal respectă principiile de protecție a datelor și cerințele legale.

10.1.4 P14S – Politica de păstrare și eliminare a datelor: se aplică oricăror date sau înregistrări partajate cu furnizorii sau stocate de aceștia și reglementează eliminarea securizată după încetarea contractului.

10.1.5 P30S – Politica de răspuns la incidente: definește modul de răspuns atunci când un furnizor cauzează sau este implicat într-un incident de securitate a informației, inclusiv procedurile de escaladare și gestionare a dovezilor.

10.2 Aceste politici funcționează împreună pentru a asigura controlul riscului asociat furnizorilor pe întreg ciclul de viață al contractului.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – impune implementarea controalelor operaționale, inclusiv a celor aplicate relațiilor cu terții și furnizorii.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.19 – asigură alinierea măsurilor de securitate ale furnizorilor la cerințele organizației.

11.2.2 Controlul 5.20 – impune acorduri formale care acoperă termenii de securitate, responsabilitățile și obligațiile în caz de încălcare.

11.2.3 Controlul 5.21 – reglementează schimbările în serviciile furnizorilor care pot afecta profilul de risc de securitate.

11.2.4 Controlul 5.22 – impune monitorizarea și revizuirea serviciilor furnizorilor și a conformității.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – reglementează achiziția de sisteme și servicii externe, impunând evaluări ale riscurilor și cerințe definite.

11.3.2 SA-10 – reglementează procedurile de configurare și schimbare care implică sisteme administrate de terți.

11.3.3 CA-3 – impune acorduri de interconectare pentru sistemele care implică entități externe.

11.3.4 PS-7 – stabilește cerințe de verificare și responsabilizare pentru personalul extern.

11.4 RGPD al UE (2016/679)

11.4.1 Articolul 28 – impune acorduri de prelucrare a datelor cu furnizorii care acționează în calitate de persoane împuternicite.

11.4.2 Articolul 32 – impune măsuri tehnice și organizatorice adecvate de securitate pentru toate persoanele împuternicite.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(a), (b), (i) – impune managementul riscurilor TIC din lanțul de aprovizionare și controale privind terții.

11.5.2 Articolul 23(1) – impune supravegherea documentată a serviciilor furnizate de terți pentru entitățile esențiale și importante.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 5(1) – impune un cadru de management al riscurilor TIC care să acopere toți furnizorii terți critici.

11.6.2 Articolul 5(2) – stabilește controale contractuale și operaționale pentru dependențele de servicii TIC.

11.6.3 Articolul 28(1), (2) – stabilește reguli de supraveghere pentru riscul asociat terților TIC în sectorul financiar.

11.7 COBIT 2019

11.7.1 APO10 – „Manage Suppliers” descrie controalele de aprovizionare și cerințele privind managementul relației cu furnizorii.

11.7.2 APO12 – „Manage Risk” integrează riscul asociat furnizorilor în guvernanța riscurilor la nivelul organizației.

11.7.3 DSS05 – „Manage Security Services” se aplică furnizorilor terți administrați și furnizorilor de servicii externalizate.