					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P27S					Titlul documentului: **Politica de utilizare a serviciilor cloud**							
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	
ISO/IEC 27002:2022	Controalele 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
GDPR	Articolul 28, 32 și capitolul V	
Directiva NIS2	Articolele 21(2)(f), (i)	
Regulamentul DORA	Articolele 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Scop

1.1 Această politică definește modul în care serviciile cloud pot fi utilizate în condiții de securitate în cadrul organizației. Aceasta asigură protejarea datelor prelucrate sau stocate în cloud, controlul accesului și gestionarea responsabilă a riscurilor.

1.2 Aceasta sprijină IMM-urile în îndeplinirea obligațiilor legale și a așteptărilor clienților privind protejarea informațiilor sensibile, prevenirea scurgerilor de date și gestionarea eficace a riscurilor asociate mediilor cloud, fără a necesita infrastructură de nivel enterprise.

1.3 Această politică sprijină certificarea ISO/IEC 27001, conformitatea cu GDPR și securitatea lanțului de aprovizionare printr-o guvernanță consecventă asupra tuturor serviciilor cloud furnizate de terți.

2. Domeniu de aplicare

2.1 Această politică se aplică următoarelor:

2.1.1 Oricărui serviciu cloud utilizat pentru stocarea, prelucrarea sau transmiterea datelor companiei

2.1.2 Întregului personal, contractorilor sau furnizorilor de servicii care utilizează instrumente cloud în numele organizației

2.1.3 Soluțiilor cloud gratuite și cu plată, inclusiv platforme de e-mail, partajare de documente, instrumente SaaS, platforme de backup, videoconferință și platforme destinate clienților

2.1.4 Oricărui dispozitiv (desktop, mobil, tabletă) care accesează informațiile companiei prin aplicații cloud

2.2 Aceasta include, fără a se limita la:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 Instrumente cloud pentru backup și recuperare în caz de dezastru

2.2.5 Foldere partajate sau aplicații utilizate pentru facturare, managementul proiectelor sau comunicarea cu clienții

3. Obiective

3.1 Prevenirea utilizării neautorizate sau cu risc ridicat a serviciilor cloud neaprobate.

3.2 Asigurarea faptului că datele sensibile sau reglementate stocate în cloud sunt protejate prin controale tehnice și organizatorice adecvate.

3.3 Definirea clară a rolurilor pentru aprobarea, configurarea, monitorizarea și scoaterea din uz a serviciilor cloud.

3.4 Controlul fluxurilor de date și aplicarea obligațiilor privind retenția, ștergerea și confidențialitatea pentru informațiile stocate în cloud.

3.5 Reducerea dependenței de conturi personale sau de instrumente fără trasabilitate prin impunerea aprobării tuturor sistemelor cloud utilizate în scopuri profesionale.

3.6 Respectarea cerințelor ISO/IEC 27001:2022, GDPR, NIS2 și DORA privind gestionarea dependențelor externe de servicii cloud.

4. Roluri și responsabilități

4.1 Director general (GM)

4.1.1 Aprobă utilizarea tuturor serviciilor cloud noi

4.1.2 Revizuiește riscurile asociate furnizorilor cloud și tipurilor de servicii

4.1.3 Asigură aplicarea politicii și supraveghează deciziile privind excepțiile

4.2 Furnizorul de suport IT sau suportul tehnic

4.2.1 Evaluează și implementează configurația securizată pentru serviciile cloud

4.2.2 Configurează conturile, controalele de acces și copiile de siguranță

4.2.3 Monitorizează respectarea cerințelor privind parolele, autentificarea multifactor și setările de securitate

[... 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 de Directorul general, în coordonare cu furnizorul de suport IT.

9.2 O revizuire formală trebuie realizată, de asemenea:

9.2.1 După un incident de securitate legat de cloud (de exemplu, breșă de securitate, pierdere de date)

9.2.2 Atunci când este introdusă o nouă platformă cloud majoră

9.2.3 Dacă se modifică cerințele legale sau de reglementare (de exemplu, actualizări GDPR, NIS2, DORA)

9.2.4 Dacă activitățile de monitorizare evidențiază utilizare necorespunzătoare sau riscuri noi

9.3 Directorul general trebuie să se asigure că:

9.3.1 Registrul serviciilor cloud este actualizat cu serviciile noi sau scoase din uz

9.3.2 Cerințele legale și de confidențialitate sunt în continuare respectate

9.3.3 Toate modificările sunt comunicate utilizatorilor relevanți și părților interesate

9.4 Versiunile arhivate trebuie stocate în condiții de securitate, iar versiunile vechi ale politicii trebuie gestionate în conformitate cu P14S – Politica de păstrare și eliminare a datelor a organizației.

10. Politici conexe și interdependențe

10.1 Această politică trebuie utilizată în corelare cu următoarele politici de securitate a informației aliniate pentru IMM-uri:

10.1.1 P2S – Politica privind rolurile și responsabilitățile de guvernanță: definește responsabilitatea pentru aprobarea serviciilor cloud și gestionarea relațiilor cu furnizorii.

10.1.2 P4S – Politica de control al accesului: sprijină practicile de autentificare securizată, gestionarea sesiunilor și revocarea accesului necesare pentru platformele cloud.

10.1.3 P14S – Politica de păstrare și eliminare a datelor: reglementează modul în care datele din cloud fac obiectul copiilor de siguranță, sunt păstrate și sunt șterse în conformitate cu obligațiile legale.

10.1.4 P17S – Politica de protecție a datelor și confidențialitate: asigură că orice date cu caracter personal stocate în servicii cloud sunt gestionate în conformitate cu principiile GDPR.

10.1.5 P30S – Politica de răspuns la incidente: oferă proceduri structurate pentru răspunsul la incidentele de securitate din cloud, inclusiv colectarea dovezilor și notificarea externă.

10.2 Împreună, aceste politici asigură că utilizarea serviciilor cloud este securizată, conformă și reziliență din punct de vedere operațional.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Impune organizațiilor să implementeze controale operaționale pentru gestionarea datelor, inclusiv a celor aferente sistemelor cloud.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.23 – Impune guvernanță asupra utilizării serviciilor cloud și a instrumentelor SaaS furnizate de terți.

11.2.2 Controlul 5.24 – Impune existența unei politici definite privind utilizarea serviciilor cloud, aliniată la risc și la cerințele de reglementare.

11.2.3 Controlul 5.25 – Impune organizațiilor să se asigure că controalele de securitate din mediile cloud răspund nevoilor organizației.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – Impune politici formale de utilizare pentru sisteme externe, cum sunt serviciile cloud.

11.3.2 SC-12, SC-13 – Vizează criptarea pentru datele în tranzit și datele în repaus în mediile cloud.

11.3.3 SR-5 – Acoperă controalele de risc privind serviciile cloud și terții din lanțul de aprovizionare.

11.4 GDPR (UE) 2016/679

11.4.1 Articolul 28 – Impune ca furnizorii cloud care acționează ca persoane împuternicite să respecte obligații contractuale obligatorii.

11.4.2 Articolul 32 – Impune controale tehnice și organizatorice pentru prelucrarea datelor în cloud.

11.4.3 Capitolul V – Interzice transferurile internaționale neautorizate ale datelor cu caracter personal stocate în cloud.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(f), (i) – Impune entităților esențiale și importante să implementeze politici adecvate pentru securitatea serviciilor cloud și controlul lanțului de aprovizionare.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 5(2) – Impune IMM-urilor din sectorul financiar să integreze securitatea cloud în cadrele lor de management al riscurilor TIC.

11.6.2 Articolul 28 – Stabilește reguli de supraveghere pentru furnizorii terți critici de servicii TIC, inclusiv furnizorii cloud.

11.7 COBIT 2019

11.7.1 DSS01 – „Manage Operations” vizează integritatea operațională a serviciilor cloud.

11.7.2 DSS05 – „Manage Security Services” include măsuri de protecție și monitorizare specifice mediilor cloud.

11.7.3 BAI04 – „Manage Availability and Capacity” asigură continuitatea activității și performanța în mediile cloud.