					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P27					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	Cerințe privind planificarea și controlul operațional pentru mediile cloud.
ISO/IEC 27002:2022	Controalele 5.23–5.25	Cerințe privind utilizarea, politica și securitatea serviciilor cloud.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12 – SC-28, SR-5	Utilizarea sistemelor externe, cerințe contractuale și tehnice, protecție criptografică, protecția lanțului de aprovizionare.
GDPR al UE	Articolele 28, 32, Capitolul V	Cerințe privind persoana împuternicită din cloud, securitatea prelucrării, transferurile de date.
Directiva NIS2 a UE	Articolul 21(2)(f, i)	Cerințe privind riscul asociat terților și lanțului de aprovizionare.
Regulamentul DORA al UE	Articolele 5(2), 28	Guvernanță și control TIC și supravegherea terților (cloud) pentru entitățile financiare.
COBIT 2019	BAI04, DSS01, DSS05	Disponibilitatea serviciilor cloud, operațiuni și managementul securității.

1. Scop

1.1 Această politică stabilește cerințele obligatorii ale organizației pentru utilizarea sigură, conformă și responsabilă a serviciilor de cloud computing în modelele de furnizare Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) și Software-as-a-Service (SaaS).

1.2 Politica are ca scop să asigure că serviciile cloud sunt adoptate și guvernate într-un mod care protejează confidențialitatea, integritatea și disponibilitatea (CIA) activelor informaționale, cu respectarea obligațiilor de reglementare, legale și contractuale.

1.3 Aceasta definește controale pentru managementul riscurilor asociate serviciilor cloud, protejarea datelor, monitorizarea conformității furnizorilor și eliminarea utilizărilor neautorizate. De asemenea, susține inovarea în activitățile organizației prin platforme cloud, prin alinierea securității, fiabilității operaționale și eficienței costurilor.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor angajaților, contractanților, furnizorilor de servicii externalizate și consultanților externi care alocă, configurează, accesează, administrează sau utilizează servicii cloud în numele organizației.

2.2 Se aplică tuturor mediilor în care sunt prelucrate datele sau sarcinile de lucru ale organizației, inclusiv:

2.2.1 implementări de cloud public, privat, hibrid și comunitar

2.2.2 toate modelele de servicii cloud (IaaS, PaaS, SaaS)

2.2.3 arhitecturi multicloud și federate

2.2.4 utilizarea shadow IT sau a conturilor cloud personale în scopuri de serviciu

2.3 Aceasta acoperă toate nivelurile de clasificare a datelor și se aplică atât sistemelor interne, cât și platformelor găzduite de furnizori, în care sunt stocate sau prelucrate date deținute de organizație ori date reglementate.

3. Obiective

3.1 Asigurarea unei utilizări sigure și consecvente a tehnologiilor cloud prin linii directoare clar definite, configurații de referință de securitate și roluri de guvernanță.

3.2 Reducerea la minimum a riscurilor operaționale și de reglementare asociate cloud computingului, inclusiv accesul neautorizat, încălcarea securității datelor, configurările eronate, neconformitatea și întreruperile serviciilor.

3.3 Impunerea cerințelor de securitate și confidențialitate pentru toți furnizorii cloud și verificarea conformității prin clauze contractuale, evaluări și drepturi de audit.

3.4 Permiterea adopției cloud scalabile și reziliente, fără a compromite profilul de risc de securitate, cerințele legale sau continuitatea activității.

3.5 Alinierea guvernanței și utilizării serviciilor cloud cu cadrul SMSI al organizației, obligațiile legale (de exemplu, GDPR, DORA), liniile directoare specifice sectorului și bunele practici recunoscute din industrie (de exemplu, NIST, COBIT).

4. Roluri și responsabilități

4.1 Conducerea executivă

4.1.1 Aprobă Politica de utilizare a serviciilor cloud și foaia de parcurs strategică pentru adopția cloud.

4.1.2 Revizuiește și aprobă excepțiile cu risc ridicat de la cerințele standard de guvernanță a serviciilor cloud.

4.1.3 Se asigură că inițiativele cloud beneficiază de finanțare adecvată, supraveghere și integrare cu cadrele de risc organizațional.

4.2 Directorul de securitate a informațiilor (CISO)

4.2.1 Este proprietarul acestei politici și al Registrului serviciilor cloud la nivelul organizației.

4.2.2 Aprobă integrarea noilor furnizori cloud pe baza verificării prealabile și a evaluării riscurilor.

4.2.3 Revizuiește documentația de conformitate a furnizorilor și validează alinierea din perspectiva securității.

[... 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 și actualizată după caz pentru a asigura alinierea continuă cu:

9.1.1 cerințele legale și de reglementare în evoluție (de exemplu, GDPR, NIS2, DORA)

9.1.2 modificările standardelor ISO/IEC 27001 sau ISO/IEC 27002

9.1.3 actualizările aduse arhitecturii cloud, peisajului de amenințări sau portofoliului de servicii al organizației

9.1.4 investigațiile incidentelor, rezultatele auditurilor sau lecțiile învățate din utilizarea operațională

9.2 CISO este responsabil pentru inițierea revizuirii și convocarea părților interesate relevante, inclusiv:

9.2.1 Arhitectul de securitate cloud

9.2.2 echipa juridică și de conformitate

9.2.3 achiziții și managerii de furnizori

9.2.4 proprietarii de servicii și operațiunile IT

9.3 Toate actualizările trebuie să fie:

9.3.1 supuse controlului versiunilor și datate

9.3.2 aprobate de conducerea executivă

9.3.3 comunicate părților afectate, inclusiv angajaților, contractanților și terților

9.3.4 arhivate în conformitate cu politicile interne de documentare

9.4 Revizuirile intermediare pot fi declanșate de:

9.4.1 noi contractări de CSP sau migrări majore

9.4.2 amenințări emergente la adresa infrastructurii cloud

9.4.3 modificări semnificative ale obligațiilor contractuale, legale sau specifice sectorului

10. Politici conexe și interdependențe

10.1 Această politică este strâns legată de următoarele politici interne și depinde de acestea:

10.1.1 P1 – Politica de securitate a informației: stabilește principiile generale care guvernează funcționarea sigură a sistemelor și serviciilor, pe care această politică le aplică în contextul cloud.

10.1.2 P5 – Politica de management al schimbărilor: toate modificările de configurație din cloud trebuie să urmeze procedurile de control al schimbărilor prevăzute în P5.

10.1.3 P13 – Politica de clasificare și etichetare a datelor: stabilește modul în care datele sunt evaluate înainte de transferul în cloud și modul în care sunt aplicate controale precum criptarea și rezidența datelor.

10.1.4 P18 – Politica privind controalele criptografice: furnizează standarde pentru criptare, managementul cheilor și utilizarea algoritmilor criptografici, aplicate direct în configurațiile serviciilor cloud.

10.1.5 P22 – Politica de jurnalizare și monitorizare: specifică cerințele pentru colectarea, păstrarea și analiza jurnalelor, care trebuie aplicate în mediile cloud.

10.1.6 P30 – Politica de răspuns la incidente: definește procedurile de escaladare, izolare și remediere pentru evenimentele de securitate legate de cloud.

10.1.7 P33 – Politica de audit și monitorizare a conformității: sprijină pregătirea pentru audit și asigurarea continuă a faptului că controalele cloud sunt aplicate și monitorizate.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001: Clauza 8.1 – Planificare și control operațional: impune organizațiilor să implementeze și să controleze procesele necesare pentru îndeplinirea cerințelor de securitate a informației, inclusiv a celor care implică medii cloud.

11.2 ISO/IEC 27002:2022 – Controalele 5.23–5.25:

11.2.1 Anexa A, Controlul 5.23 – Utilizarea serviciilor cloud: impune evaluarea bazată pe risc, autorizarea formală și documentarea utilizării serviciilor cloud.

11.2.2 Anexa A, Controlul 5.24 – Politica privind utilizarea serviciilor cloud: impune stabilirea și aplicarea politicilor formale de utilizare a serviciilor cloud, aliniate la nevoile și riscurile organizației.

11.2.3 Anexa A, Controlul 5.25 – Securitatea în serviciile cloud: impune integrarea securității, protecțiilor contractuale și monitorizarea sarcinilor de lucru și a datelor găzduite în cloud.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – Utilizarea sistemelor externe: impune reguli și condiții definite pentru accesarea resurselor organizației din sisteme externe sau din cloud.

11.3.2 SA-9(5) – Servicii ale sistemelor informatice externe: impune cerințe contractuale de securitate, supraveghere și monitorizare continuă pentru sistemele cloud ale terților.

11.3.3 SC-12 până la SC-28 – Protecție criptografică, apărarea perimetrului și integritatea transmisiilor: se aliniază cerințelor privind criptarea, identitatea și accesul pentru serviciile găzduite în cloud și datele în tranzit.

11.3.4 SR-5 – Protecția lanțului de aprovizionare: susține evaluarea și controlul contractual asupra CSP-urilor implicate în furnizarea serviciilor.

11.4 GDPR al UE (2016/679):

11.4.1 Articolul 28 – Obligațiile persoanei împuternicite: impune contracte formale cu furnizorii cloud pentru a asigura securitatea, confidențialitatea și caracterul verificabil al prelucrării datelor cu caracter personal.

11.4.2 Articolul 32 – Securitatea prelucrării: susține aplicarea criptării, controalelor de acces, jurnalizării și altor măsuri de protecție în mediile cloud.

11.4.3 Capitolul V – Transferuri internaționale de date: impune transferul legal al datelor în afara UE/SEE utilizând măsuri de protecție precum clauze contractuale standard (SCC) sau decizii de adecvare.

11.5 Directiva NIS2 a UE (2022/2555):

11.5.1 Articolul 21(2)(f, i): impune entităților să gestioneze riscurile provenite de la furnizorii terți de servicii cloud și să asigure integritatea lanțului digital de aprovizionare prin măsuri contractuale și tehnice.

11.6 DORA a UE (2022/2554):

11.6.1 Articolul 5(2) – Guvernanța riscurilor TIC: impune integrarea riscului TIC asociat terților, inclusiv serviciilor cloud, în guvernanța generală a riscurilor.

11.6.2 Articolul 28 – Supravegherea furnizorilor terți critici de servicii TIC: impune entităților financiare să monitorizeze, să controleze și să raporteze dependențele de furnizorii cloud, profilul de risc și reziliența acestora.

11.7 COBIT 2019:

11.7.1 BAI04 – Gestionarea disponibilității și capacității: asigură că serviciile cloud sunt reziliente, monitorizate și îndeplinesc criteriile de performanță definite.

11.7.2 DSS01 – Gestionarea operațiunilor: susține integrarea operațională, tratarea incidentelor și configurațiile de referință în toate platformele găzduite în cloud.

11.7.3 DSS05 – Gestionarea serviciilor de securitate: orientează implementarea controalelor de securitate specifice cloudului, monitorizarea și prevenirea incidentelor în cadrul serviciilor digitale.