					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P03					Titlul documentului: **Politica de utilizare acceptabilă**							
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 standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 5	Stabilește norme de comportament și cerințe pentru Politica de utilizare acceptabilă
ISO/IEC 27002:2022	Controalele 6.1, 6.2, 8.1, 8.12	Oferă orientări privind responsabilitățile în domeniul securității informației, conștientizarea și guvernanța dispozitivelor și a datelor
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Controale de acces și controale de conștientizare/comportament relevante pentru utilizarea activelor IT
GDPR al UE	Articolele 5(1)(f), 32; Considerentul 39	Impune confidențialitatea și integritatea, măsuri tehnice și organizatorice și temeiuri legale pentru utilizarea adecvată
Directiva NIS2 a UE	Articolul 21(2)(a–d)	Impune politici operaționale și instruire pentru utilizarea securizată
Regulamentul DORA al UE	Articolul 5	Susține managementul riscurilor TIC prin reglementarea comportamentului utilizatorilor
COBIT 2019	APO07, BAI05, DSS05, MEA01	Resurse umane, managementul schimbării, servicii de securitate gestionate, monitorizarea conformității și performanței

1. Scop

1.1 Această politică definește utilizarea acceptabilă și utilizarea inacceptabilă a sistemelor informatice ale organizației, a resurselor de calcul, a instrumentelor de comunicare și a practicilor de gestionare a datelor.

1.2 Aceasta asigură că toți utilizatorii își înțeleg responsabilitățile atunci când utilizează activele IT ale organizației și că acțiunile lor susțin confidențialitatea, integritatea, disponibilitatea (CIA) și prelucrarea legală a informațiilor.

1.3 Politica îndeplinește cerințele ISO/IEC 27001:2022, Clauza 5.10, prin stabilirea normelor de comportament pentru utilizarea sistemelor și prin aplicarea de măsuri de protecție tehnice și procedurale pentru a reduce la minimum riscul de utilizare abuzivă, neglijență sau utilizare necorespunzătoare.

1.4 De asemenea, aceasta sprijină activitățile de investigare și aplicare, inclusiv răspunsul la incidente și măsurile disciplinare pentru încălcări.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor persoanelor și entităților cărora li se acordă acces la sistemele informatice și activele organizației, inclusiv, dar fără a se limita la:

2.1.1 Angajați, contractori, consultanți, stagiari și personal pus la dispoziție prin agenții

2.1.2 Furnizori terți care au acces la sisteme sau roluri administrative delegate

2.1.3 Vizitatori sau parteneri care utilizează infrastructură IT deținută de organizație sau autorizată de aceasta

2.2 Domeniul de aplicare include toate activele tehnologice și de date ale organizației, inclusiv:

2.2.1 Stații de lucru, laptopuri, dispozitive mobile și servere

2.2.2 Infrastructură de rețea și servicii cloud

2.2.3 E-mail, mesagerie, stocare de fișiere, platforme de colaborare și VPN-uri

2.2.4 Date în repaus, în tranzit sau în curs de prelucrare, indiferent de format sau locație

2.2.5 Orice dispozitiv personal utilizat în cadrul unui program Bring Your Own Device (BYOD) care se conectează la sistemele organizației

2.3 Această politică se aplică în toate mediile de lucru, inclusiv:

2.3.1 Birouri corporative și locații de producție

2.3.2 Locații de telemuncă sau configurații hibride

2.3.3 Operațiuni desfășurate pe teren sau spații administrate de terți

2.4 Toți utilizatorii au obligația să confirme luarea la cunoștință și să respecte această politică drept condiție pentru accesarea sistemelor companiei sau gestionarea datelor corporative.

3. Obiective

3.1 Să definească și să impună reguli privind utilizarea acceptabilă a resurselor IT ale organizației.

3.2 Să prevină accesul neautorizat, scurgerile de date și prejudiciile rezultate din utilizarea neglijentă sau malițioasă.

3.3 Să protejeze rețelele, activele și datele companiei împotriva amenințărilor generate de comportamentul utilizatorilor.

3.4 Să susțină obligațiile legale și contractuale prin demonstrarea diligenței necesare în guvernanța resurselor IT.

3.5 Să asigure consecvență și claritate în aplicarea măsurilor disciplinare și a proceselor de gestionare a excepțiilor.

3.6 Să promoveze o cultură a utilizării etice, securizate și responsabile a resurselor digitale și fizice de calcul.

4. Roluri și responsabilități

4.1 Conducerea executivă

4.1.1 Aprobă Politica de utilizare acceptabilă și se asigură că aceasta este aliniată la obiectivele de afaceri, cerințele de reglementare și valorile organizației.

4.1.2 Alocă resurse pentru aplicare, instruire, monitorizare și revizuirea politicii.

4.1.3 Revizuiește stadiul conformității și măsurile disciplinare asociate încălcărilor politicii, ca parte a guvernanței SMSI.

4.2 Echipele IT și de securitate a informațiilor

4.2.1 Implementează măsuri de protecție tehnice pentru aplicarea acestei politici, inclusiv:

4.2.2 Filtrarea conținutului, protecția antimalware, securitatea punctelor terminale și instrumente de monitorizare a rețelei

4.2.3 Configurații de securitate a poștei electronice și soluții de prevenire a pierderii datelor (DLP)

4.2.4 Liste de blocare și liste de permitere pentru software, hardware și site-uri web

4.2.5 Mențin un inventar al software-ului, dispozitivelor și serviciilor aprobate și interzise.

4.2.6 Investighează suspiciunile de încălcare a Politicii de utilizare acceptabilă, colectează probe criminalistice și sprijină acțiunile disciplinare sau juridice, după caz.

4.2.7 Colaborează cu Resursele Umane și funcția juridică în gestionarea incidentelor, escaladare și îndeplinirea obligațiilor de raportare.

[... 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 Declanșatori ai revizuirii și frecvență

9.1.1 Această politică trebuie revizuită:

9.1.1.1 Cel puțin anual

9.1.1.2 În urma oricăror schimbări semnificative de tehnologie sau infrastructură

9.1.1.3 După incidente sau constatări de audit care evidențiază lacune în aplicare

9.1.1.4 Ca răspuns la modificări ale legislației aplicabile sau ale obligațiilor contractuale

9.2 Deținere și aprobare

9.2.1 Directorul de securitate a informațiilor sau Managerul SMSI desemnat este responsabil pentru procesul de revizuire.

9.2.2 Actualizările trebuie aprobate de conducerea executivă și comunicate la nivelul întregii organizații.

9.2.3 Confirmarea luării la cunoștință a termenilor actualizați trebuie obținută din nou la republicarea politicii.

9.3 Managementul documentului

9.3.1 Politica trebuie să includă următoarele metadate și detalii de versionare:

9.3.1.1 Titlul, ID-ul și nivelul de clasificare

9.3.1.2 Proprietarul politicii și responsabilul cu administrarea documentului

9.3.1.3 Istoricul modificărilor și justificarea actualizărilor

9.3.1.4 Datele revizuirii și ale următoarei actualizări planificate

9.3.1.5 Referințe la jurnalul de distribuire și de confirmare a luării la cunoștință

9.3.2 Exemplarul principal trebuie păstrat în depozitul de documente al SMSI, sub controlul versiunilor.

10. Politici conexe și corelări

10.1 Această politică trebuie interpretată împreună cu următoarele:

10.1.1 P1 – Politica de securitate a informației: stabilește așteptările de bază privind comportamentul și angajamentul conducerii de vârf față de utilizarea acceptabilă.

10.1.2 P4 – Politica de control al accesului: definește permisiunile și drepturile asociate utilizatorilor, sistemelor și accesului la date, aplicând în mod direct limitele utilizării acceptabile.

10.1.3 P6 – Politica de management al riscurilor: tratează riscurile asociate comportamentului și susține activitățile de monitorizare și tratament asociate amenințărilor generate de utilizatori.

10.1.4 P7 – Politica de integrare și încetare a personalului: asigură confirmarea luării la cunoștință a condițiilor de utilizare acceptabilă la intrare și revocarea acestora la plecare.

10.1.5 P9 – Politica de telemuncă: extinde prevederile privind utilizarea acceptabilă la mediile de lucru la distanță și hibride.

10.2 Aceste politici conexe formează un model de apărare stratificat pentru guvernanța comportamentală, tehnică și contractuală.

11. Standarde și cadre de referință

11.1 Această Politică de utilizare acceptabilă este aliniată la standarde recunoscute la nivel internațional și la cadre juridice relevante pentru a asigura controale comportamentale aplicabile, verificabile și bazate pe risc pentru toate situațiile de utilizare a sistemelor informaționale digitale și fizice.

11.2 ISO/IEC 27001:2022

11.2.1 Clauza 5.10 – Utilizarea acceptabilă a informațiilor și a altor active asociate: această politică îndeplinește în mod direct cerința de a defini, comunica și impune reguli care guvernează utilizarea adecvată a resurselor IT.

11.2.2 Anexa A, Controlul 6.1 – Responsabilitatea pentru securitatea informației: atribuie responsabilități clare pentru comportamentul utilizatorilor și supravegherea conformității.

11.2.3 Anexa A, Controlul 6.2 – Conștientizare, educație și instruire în domeniul securității informației: procesele integrate de instruire și de confirmare a politicii fac parte din aplicarea Politicii de utilizare acceptabilă.

11.2.4 Anexa A, Controlul 8.1 – Dispozitive punct terminal ale utilizatorilor și 8.12 – Prevenirea pierderii datelor: tratează comportamentul acceptabil pe dispozitivele utilizatorilor și guvernează activitățile care ar putea conduce la expunerea sau scurgerea datelor.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Controlul accesului pentru dispozitive mobile) și AC-20 (Utilizarea sistemelor informaționale externe): această politică definește obligațiile și restricțiile utilizatorilor pentru BYOD și accesul la sisteme ale terților.

11.3.2 PL-4 (Reguli de comportament): oferă cerințe detaliate privind utilizarea acceptabilă, în concordanță cu această politică.

11.3.3 AT-2 (Instruire de conștientizare a securității): este susținut prin instruirea utilizatorilor și prin confirmarea documentată a politicii.

11.3.4 AU-2 (Evenimente de audit) și AU-12 (Generarea înregistrărilor de audit): aplicarea se bazează pe monitorizarea acțiunilor utilizatorilor și alertarea privind încălcările.

11.4 GDPR al UE (2016/679):

11.4.1 Articolul 5(1)(f): impune securitatea și integritatea datelor cu caracter personal; această politică reduce riscurile introduse de comportamentul uman și de utilizarea neautorizată.

11.4.2 Articolul 32: impune măsuri tehnice și organizatorice, cum ar fi controalele comportamentale și restricțiile de utilizare, pentru protejarea datelor cu caracter personal.

11.4.3 Considerentul 39: evidențiază necesitatea de a asigura doar accesul necesar și utilizarea legală a datelor de către persoane autorizate.

11.5 Directiva NIS2 a UE (2022/2555):

11.5.1 Articolul 21(2)(a–d): solicită politici operaționale și instruire pentru utilizarea securizată a sistemelor, pe care această Politică de utilizare acceptabilă le furnizează prin definirea comportamentului, a monitorizării și a proceselor de aplicare.

11.6 Regulamentul DORA al UE (2022/2554):

11.6.1 Articolul 5: această politică susține cadrul de management al riscurilor TIC prin definirea regulilor pentru interacțiunea om-sistem și prin reducerea la minimum a expunerii la riscuri cibernetice bazate pe comportament.

11.7 COBIT 2019:

11.7.1 APO07 – Gestionarea resurselor umane: impune responsabilitățile utilizatorilor și conștientizarea pe întreg ciclul de viață al angajatului.

11.7.2 BAI05 – Gestionarea schimbării organizaționale: integrează guvernanța utilizării acceptabile în procesele de schimbare care afectează comportamentul utilizatorilor.

11.7.3 DSS05 – Servicii de securitate gestionate: susține monitorizarea activităților utilizatorilor, alertele comportamentale și mecanismele automate de răspuns.

11.7.4 MEA01 – Măsurarea, evaluarea și analiza performanței și conformității: politica definește metrici și mecanisme pentru validarea conformității utilizatorilor cu așteptările comportamentale.