					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P03S					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**

Aliniere la standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauza 5	Relevantă pentru domeniul general de aplicare al politicii și pentru implementare
ISO/IEC 27002:2022	5.10, 5.11, 5	Ghid privind cerințele și controalele referitoare la utilizarea acceptabilă
NIST SP 800-53 Rev. 5	AC-19, AC-20, AT-2	Acoperă utilizarea sistemelor/dispozitivelor, monitorizarea și instruirea utilizatorilor
RGPD al UE	Articolele 5 alin. (1) lit. (f), 32	Integritatea și confidențialitatea datelor, precum și măsurile de securitate
Directiva NIS2 a UE	Articolul 21 alin. (2) lit. (b)	Impune politici adecvate de securitate și privind utilizarea acceptabilă
Regulamentul DORA al UE	Articolul 9	Politica de management al riscurilor TIC, controale, aplicare
COBIT 2019	DSS05, BAI08	Servicii de securitate și managementul cunoștințelor

1. Scop

1.1. Această politică definește utilizarea acceptabilă, responsabilă și sigură a sistemelor, dispozitivelor, accesului la internet, poștei electronice, serviciilor cloud și a oricăror dispozitive personale utilizate în scop profesional, puse la dispoziție de companie sau aprobate pentru utilizare în activitățile organizației.

1.2. Aceasta asigură că persoanele vizate înțeleg obligațiile care le revin atunci când utilizează resursele IT ale organizației, protejând integritatea datelor, confidențialitatea și continuitatea activității.

1.3. Această politică sprijină conformitatea cu ISO/IEC 27001:2022 prin impunerea unor standarde clare de conduită pentru utilizatori, aliniate cu cerințele legale, contractuale și de reglementare.

2. Domeniu de aplicare

2.1. Această politică se aplică tuturor persoanelor care accesează, administrează sau utilizează sistemele ori datele companiei, inclusiv:

2.1.1. Angajaților și contractorilor

2.1.2. Lucrătorilor temporari sau stagiarilor

2.1.3. Furnizorilor externi de servicii IT

2.2. Politica acoperă:

2.2.1. Calculatoarele, telefoanele și tabletele deținute de companie

2.2.2. Dispozitivele personale aprobate pentru utilizare în scop profesional (BYOD)

2.2.3. Rețelele companiei, platformele cloud și serviciile software

2.2.4. Accesul la internet, sistemele de poștă electronică, spațiile de stocare partajate și aplicațiile de business

2.3. Această politică se aplică în toate mediile de lucru — la sediu, la distanță și hibride — precum și pe întreaga durată a programului de lucru.

3. Obiective

3.1. Să definească ce constituie utilizarea acceptabilă și inacceptabilă a sistemelor IT.

3.1.1. Să reducă riscurile de securitate generate de utilizarea necorespunzătoare, accesul neautorizat sau introducerea de malware.

3.1.2. Să protejeze datele de business, informațiile despre clienți și reputația companiei.

3.1.3. Să stabilească reguli obligatorii și să asigure răspunderea tuturor utilizatorilor.

3.1.4. Să sprijine monitorizarea și conformitatea pentru detectarea timpurie a încălcărilor și adoptarea măsurilor corective.

4. Roluri și responsabilități

4.1. Directorul general

4.1.1. Aprobă această politică și răspunde de asigurarea resurselor și autorității necesare pentru aplicarea acesteia.

4.1.2. Revizuiește și autorizează orice excepții de la această politică.

4.2. Managerul IT sau furnizorul extern de servicii IT

4.2.1. Menține inventarele aprobate de software și hardware.

4.2.2. Configurează dispozitivele pentru aplicarea regulilor privind utilizarea acceptabilă (de exemplu, filtrarea conținutului, jurnale de acces).

4.2.3. Monitorizează utilizarea în vederea identificării potențialelor încălcări și investighează incidentele.

4.2.4. Asigură că dispozitivele personale (BYOD) sunt autorizate și securizate dacă sunt utilizate în scop profesional.

[... 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. Revizuire anuală

9.1.1. Această politică trebuie revizuită anual de Managerul IT, cu aprobarea finală a Directorului general, pentru a se asigura că rămâne aliniată cu tiparele de utilizare a tehnologiei, riscurile emergente și obligațiile de conformitate.

9.2. Declanșatori pentru revizuiri intermediare

9.2.1. Revizuirile trebuie efectuate și ca răspuns la:

9.2.2. Sisteme sau tehnologii noi (de exemplu, un nou serviciu cloud sau o nouă platformă pentru terminale)

9.2.3. Încălcări semnificative ale politicii

9.2.4. Modificări ale legislației sau ale termenilor contractuali care afectează utilizarea IT

9.3. Documentarea modificărilor

9.3.1. Toate actualizările trebuie înregistrate într-un jurnal al versiunilor care include:

9.3.1.1. Numărul versiunii

9.3.1.2. Data revizuirii

9.3.1.3. Rezumatul modificărilor

9.3.1.4. Autoritatea de aprobare

9.4. Comunicarea politicii

9.4.1. Versiunile revizuite ale acestei politici trebuie comunicate tuturor utilizatorilor afectați. Angajații trebuie să confirme primirea și înțelegerea acesteia ca parte a obligațiilor lor de conștientizare în domeniul securității.

10. Politici conexe și corelări

10.1. Această politică se aplică împreună cu alte politici SME pentru a asigura acoperirea completă a responsabilităților de securitate:

10.1.1. P4S – Politica de control al accesului: Definește aplicarea tehnică și procedurală a utilizării permise și a restricțiilor privind conturile.

10.1.2. P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: Oferă instruirea utilizatorilor privind limitele utilizării acceptabile și obligațiile de raportare.

10.1.3. P9S – Politica de telemuncă: Reglementează utilizarea sistemelor companiei în afara sediului sau din mediul de acasă.

10.1.4. P17S – Politica de protecție a datelor și confidențialitate: Impune reguli de gestionare a datelor cu caracter personal care se intersectează cu monitorizarea utilizării acceptabile și BYOD.

10.1.5. P30S – Politica de răspuns la incidente: Reglementează procedurile de investigare și răspuns la utilizarea necorespunzătoare sau la încălcările condițiilor de utilizare acceptabilă.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 5.10 – Impune organizațiilor să definească și să aplice utilizarea acceptabilă a activelor informaționale.

11.2. ISO/IEC 27002

11.2.1. Controlul 5.10 – Oferă orientări privind utilizarea acceptabilă a sistemelor, inclusiv comportamentele permise și interzise.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-19 – Abordează controlul utilizării sistemelor, inclusiv al dispozitivelor personale.

11.3.2. AC-20 – Impune autorizarea și monitorizarea sistemelor externe.

11.3.3. AT-2 – Evidențiază instruirea utilizatorilor privind practicile de utilizare acceptabilă.

11.4. RGPD al UE

11.4.1. Articolul 5 alin. (1) lit. (f) – Impune integritatea și confidențialitatea datelor cu caracter personal, care pot fi compromise prin utilizarea necorespunzătoare de către utilizatori.

11.4.2. Articolul 32 – Impune implementarea de măsuri tehnice și organizatorice pentru securizarea sistemelor și datelor.

11.5. Directiva NIS2 a UE

11.5.1. Articolul 21 alin. (2) lit. (b) – Impune politici de securitate adecvate, inclusiv reguli privind utilizarea acceptabilă, pentru atenuarea amenințărilor cibernetice.

11.6. Regulamentul DORA al UE

11.6.1. Articolul 9 – Impune politici de management al riscurilor TIC, care includ controale de utilizare și mecanisme de aplicare.

11.7. COBIT 2019

11.7.1. DSS05 – Gestionarea serviciilor de securitate: subliniază controlul bazat pe politici asupra comportamentului utilizatorilor.

11.7.2. BAI08 – Gestionarea cunoștințelor: abordează conștientizarea responsabilităților prevăzute de politici și instruirea privind utilizarea acceptabilă.