					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P08S					Titlul documentului: **Politica privind conștientizarea și instruirea în domeniul securității informației**							
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 7	
ISO/IEC 27002:2022	Control 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Directiva UE NIS2	Articolul 21 alineatul (2) litera (i)	
Regulamentul UE DORA	Articolul 13	
COBIT 2019	BAI08, DSS	
GDPR	Articolele 32, 39	

1. Scop

1.1. Prezenta politică asigură că toți angajații și contractanții își înțeleg responsabilitățile privind securitatea informației.

1.2. Aceasta are ca scop reducerea probabilității erorii umane, îmbunătățirea capacității de detectare și raportare a incidentelor și consolidarea unei culturi orientate către securitate la nivelul întregii organizații.

1.3. Politica sprijină conformitatea cu ISO/IEC 27001, NIS2, GDPR și DORA prin integrarea conștientizării securității în activitatea curentă și în responsabilitățile asociate rolurilor.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică tuturor angajaților, contractanților, stagiarilor și terților care au acces la sistemele sau datele companiei.

2.2. Aceasta include:

2.2.1. instruirea introductivă de conștientizare în domeniul securității, la angajare, pentru personalul nou

2.2.2. instruirea anuală de reîmprospătare în domeniul securității

2.2.3. activități ad-hoc de conștientizare (de exemplu, actualizări legate de incidente, afișe sau recomandări)

2.3. Se aplică tuturor rolurilor, departamentelor și locațiilor de lucru.

3. Obiective

3.1. Să asigure că întregul personal primește la timp instruire privind conștientizarea securității informației, într-un format clar și relevant.

3.2. Să ofere angajaților capacitatea de a identifica și evita amenințările uzuale, precum atacurile de tip phishing, programele malware și scurgerile de date.

3.3. Să asigure documentarea finalizării instruirii pentru a demonstra conformitatea cu cerințele legale, contractuale și de audit.

3.4. Să mențină conținutul instruirii actualizat, astfel încât acesta să reflecte politicile organizației, amenințările și reglementările aplicabile.

3.5. Să încurajeze în rândul personalului o abordare proactivă, în care securitatea este considerată parte a responsabilității zilnice.

4. Roluri și responsabilități

4.1. Director general

4.1.1. Aprobă cerințele de instruire și se asigură că sunt alocate resursele necesare.

4.1.2. Revizuiește rapoartele privind finalizarea instruirii și escaladează cazurile de neconformitate, dacă este necesar.

4.2. Manager administrativ / Resurse umane

4.2.1. Coordonează desfășurarea instruirii pentru noii angajați și a instruirii anuale de reîmprospătare.

4.2.2. Menține evidențele de instruire și registrele privind finalizarea instruirii.

4.2.3. Se asigură că personalul confirmă luarea la cunoștință a politicilor esențiale de securitate a informației și a acordurilor de confidențialitate (NDA).

[... 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. Prezenta politică trebuie revizuită anual de Directorul general și Resursele umane pentru a se asigura că reflectă riscurile curente, reglementările aplicabile și nevoile forței de muncă.

9.2. Actualizări intermediare

9.2.1. Politica și conținutul instruirii trebuie, de asemenea, revizuite și actualizate după:

9.2.1.1. un incident de securitate semnificativ

9.2.1.2. modificări legale sau contractuale

9.2.1.3. restructurări organizaționale sau migrări de sisteme

9.3. Controlul versiunilor și distribuirea

9.3.1. Fiecare actualizare trebuie să includă:

9.3.1.1. numărul versiunii și data intrării în vigoare

9.3.1.2. rezumatul modificărilor

9.3.1.3. aprobarea Directorului general

9.3.1.4. arhiva tuturor versiunilor anterioare, păstrată pentru cel puțin trei ani

9.4. Comunicarea către angajați

9.4.1. Actualizările politicii trebuie comunicate întregului personal, iar confirmarea de luare la cunoștință trebuie obținută dacă sunt introduse modificări semnificative.

10. Politici conexe și corelări

10.1. Prezenta politică sprijină următoarele documente:

10.1.1. P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește responsabilitatea pentru coordonarea și supravegherea instruirii

10.1.2. P3S – Politica de utilizare acceptabilă: consolidează așteptările privind comportamentul abordate în instruire

10.1.3. P4S – Politica de control al accesului: asigură că utilizatorii înțeleg importanța securității accesului

10.1.4. P7S – Politica de integrare și încetare a raporturilor de muncă: integrează instruirea în procesul de intrare în organizație

10.1.5. P30S – Politica de răspuns la incidente: asigură că personalul știe cum să raporteze prompt și corect incidentele

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 7.3 – impune organizațiilor să se asigure că personalul este conștient de responsabilitățile sale și de impactul asupra securității

11.2. ISO/IEC 27002

11.2.1. Control 6.3 – detaliază cerințele privind domeniul și modalitatea de desfășurare a instruirii de securitate

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – impune instruire de conștientizare pentru utilizatorii cu acces la sisteme

11.3.2. AT-4 – acoperă instruirea bazată pe roluri și consecințele neconformității

11.4. GDPR

11.4.1. Articolul 32 – impune măsuri de securitate, inclusiv instruirea personalului, pentru protejarea datelor cu caracter personal

11.4.2. Articolul 39 – impune ca responsabilul cu protecția datelor (DPO) să supravegheze activitățile de conștientizare și instruire, după caz

11.5. Directiva UE NIS2

11.5.1. Articolul 21 alineatul (2) litera (i) – impune programe continue de conștientizare și instruire în domeniul securității cibernetice

11.6. Regulamentul UE DORA

11.6.1. Articolul 13 – impune entităților financiare să implementeze activități de educare și instruire pentru întregul personal cu responsabilități legate de TIC

11.7. COBIT 2019

11.7.1. BAI08 – Managementul cunoștințelor: asigură că personalul este competent și instruit

11.7.2. DSS05 – Managementul serviciilor de securitate: evidențiază conștientizarea ca măsură de protecție esențială