| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Introduceți aici denumirea entității juridice înregistrate | | | | | | | |
| Numărul documentului:<br>P08 | | | | | Titlul documentului:<br>**Politica privind conștientizarea și instruirea în domeniul securității informației** | | | | | | | |
| Versiunea:<br>1.0 | | Data intrării în vigoare:<br>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 7.3, Anexa A Controlul 6.3 | Stabilește cerințele privind conștientizarea și instruirea abordate prin această politică |
| ISO/IEC 27002:2022 | Controlul 6 | Susține instruirea adecvată de conștientizare, bazată pe rol |
| GDPR al UE | Articolele 32, 39; Considerentul 78 | Impune instruirea persoanelor care prelucrează date cu caracter personal și conștientizarea generală a personalului |
| Directiva NIS2 a UE | Articolele 21(2)(a, b), 21(3) | Impune politici de instruire privind riscurile și securitatea, precum și inițiative de conștientizare |
| Regulamentul DORA al UE | Articolele 5, 8, 13 | Impune conștientizarea riscurilor TIC și instruirea ca parte a controalelor de reziliență |
| COBIT 2019 | APO07, DSS05, MEA | Consolidează conștientizarea personalului, instruirea utilizatorilor și monitorizarea conformității |
| NIST SP 800-53 Rev.5 | AT-1 până la AT-5 | Se aliniază cu politica și procedurile, instruirea de conștientizare, instruirea bazată pe rol, evidențele de instruire și contactul cu grupurile de securitate |

## 1. Scop

1.1 Această politică stabilește cadrul formal pentru a asigura că întregul personal este conștient de responsabilitățile sale privind securitatea informației și primește instruirea necesară pentru a proteja confidențialitatea, integritatea și disponibilitatea activelor informaționale.

1.2 Această politică sprijină Clauza 7.3 din ISO/IEC 27001 și Controlul 6.3 din Anexa A prin impunerea unui program structurat de conștientizare și instruire, bazat pe risc, adaptat rolurilor din organizație și amenințărilor în evoluție.

1.3 Politica contribuie la reducerea vulnerabilităților de natură umană, la promovarea unui comportament orientat spre securitate și la consolidarea continuă a practicilor sigure, în conformitate cu cerințele de reglementare și contractuale.

## 2. Domeniu de aplicare

**2.1 Această politică se aplică tuturor persoanelor interne și externe care au acces la sistemele informatice ale organizației, la date sau la facilități, inclusiv:**

2.1.1 angajați (cu normă întreagă, cu normă parțială, temporari)

2.1.2 contractori, consultanți, furnizori și stagiari

2.1.3 terți cu acces logic sau fizic în baza acordurilor privind nivelul serviciilor (SLA)

**2.2 Domeniul de aplicare include:**

2.2.1 instruirea inițială de conștientizare în domeniul securității la angajare

2.2.2 instruirea specifică rolului (de exemplu, dezvoltatori, personal financiar, utilizatori privilegiați)

2.2.3 instruirea periodică de reîmprospătare și programele de conștientizare

2.2.4 instruirea ad hoc ca răspuns la incidente sau amenințări noi

2.3 Metodele de livrare a instruirii acoperite de această politică includ e-learning, sesiuni față în față, simulări, teste de cunoștințe, postere, buletine informative și confirmări obligatorii.

**3. Obiective**

3.1 Să asigure că întregul personal își înțelege responsabilitățile privind protejarea activelor organizației și respectarea politicilor de securitate.

3.2 Să furnizeze instruire continuă și măsurabilă în materie de conștientizare, aliniată la expunerea la risc specifică rolurilor.

3.3 Să integreze comportamente sigure în activitățile zilnice prin consolidarea unor practici precum utilizarea sigură a parolelor, raportarea și gestionarea incidentelor și rezistența la atacuri de tip phishing.

3.4 Să asigure conformitatea cu reglementările și pregătirea pentru audit în raport cu obligațiile de instruire în domeniul securității informației din diferite industrii și jurisdicții.

3.5 Să reducă incidentele de securitate rezultate din neglijență, lipsă de conștientizare sau erori de judecată prin formarea comportamentelor și consolidarea continuă a acestora.

**4. Roluri și responsabilități**

**4.1 Managementul executiv**

4.1.1 Aprobă strategia organizației privind instruirea în domeniul securității informației și se asigură că aceasta beneficiază de resurse adecvate și este integrată în prioritățile corporative.

4.1.2 Monitorizează conformitatea la nivel managerial și asigură respectarea politicii în toate departamentele.

**4.2 Directorul de securitate a informațiilor / Managerul de securitate a informațiilor**

4.2.1 Deține această politică și definește cadrul de conștientizare și instruire în conformitate cu riscurile, cerințele de conformitate și nevoile organizației.

4.2.2 Supraveghează proiectarea, livrarea, monitorizarea și revizuirea tuturor inițiativelor de instruire în domeniul securității.

4.2.3 Se asigură că instruirea este actualizată periodic și reflectă amenințările în evoluție și tehnologiile emergente.

[ ... 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 Frecvența revizuirii**

**9.1.1 Această politică și programul de instruire asociat trebuie revizuite:**

9.1.1.1 anual, sau

9.1.1.2 după incidente majore care implică eroare umană sau amenințări interne

9.1.1.3 la introducerea unor tehnologii sau amenințări noi semnificative

9.1.1.4 ca răspuns la modificări ale obligațiilor legale, contractuale sau de certificare

**9.2 Procesul de revizuire**

**9.2.1 Revizuirea trebuie coordonată de Directorul de securitate a informațiilor, în colaborare cu:**

9.2.1.1 Resurse umane și departamentele de instruire

9.2.1.2 responsabilii juridici și responsabilii cu protecția datelor

9.2.1.3 funcțiile de securitate IT și risc operațional

**9.2.2 Toate actualizările trebuie:**

9.2.2.1 aprobate de Comitetul de coordonare al SMSI

9.2.2.2 gestionate prin controlul versiunilor și documentate în Registrul documentelor SMSI

9.2.2.3 comunicate utilizatorilor dacă modificările semnificative afectează domeniul de aplicare al instruirii sau responsabilitățile

**9.3 Guvernanța actualizării conținutului**

**9.3.1 Modulele de instruire și materialele de conștientizare trebuie revizuite la fiecare 12 luni pentru a asigura:**

9.3.1.1 relevanța pentru peisajul amenințărilor

9.3.1.2 acuratețea din perspectiva reglementărilor

9.3.1.3 compatibilitatea formatului (de exemplu, accesibilitate, localizare)

9.3.2 Conținutul depășit sau care poate induce în eroare trebuie retras imediat și înlocuit cu alternative aprobate.

## 10. Politici corelate și interdependențe

**10.1 Această politică este susținută de următoarele politici și sprijină aplicarea acestora:**

10.1.1 P01 – Politica de securitate a informației: stabilește conștientizarea securității ca un control fundamental în Sistemul de management al securității informației (SMSI) al organizației.

10.1.2 P03 – Politica de utilizare acceptabilă: impune confirmarea de către utilizator în cadrul instruirii și clarifică responsabilitățile asociate utilizării zilnice a tehnologiei.

10.1.3 P07 – Politica de integrare și încetare a personalului: asigură integrarea instruirii la intrare și monitorizarea acesteia pe toată durata raportului de muncă.

10.1.4 P06 – Politica de management al riscurilor: corelează instruirea centrată pe factorul uman cu modelarea amenințărilor și strategiile de reducere a riscului rezidual.

10.1.5 P33 – Politica de audit și monitorizare a conformității: validează faptul că măsurile de conștientizare sunt operaționale, măsurabile și eficace în timpul auditurilor.

10.2 Împreună, aceste politici formează un cadru cuprinzător de control comportamental care integrează conștientizarea, responsabilizarea și consolidarea culturii organizaționale.

## 11. Standarde și cadre de referință

**11.1 ISO/IEC 27001**

11.1.1 Clauza 7.3 – Conștientizare: impune organizațiilor să se asigure că lucrătorii sunt conștienți de politicile de securitate a informației și de responsabilitățile lor. Această politică operationalizează această cerință prin onboarding structurat, instruire periodică și participare măsurabilă la campanii.

11.1.2 Anexa A Controlul 6.3 – Conștientizare, educație și instruire în domeniul securității informației: este abordată integral prin programe de instruire inițială, bazată pe rol și continuă, adaptate profilurilor de risc ale utilizatorilor.

**11.2 ISO/IEC 27002:2022 – Controlul 6**

11.2.1 Sprijină dezvoltarea și livrarea instruirii de conștientizare adecvate rolurilor profesionale, cu accent pe consolidarea comportamentului sigur și pe actualizări periodice bazate pe informații privind amenințările și feedbackul din audit.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AT-1 până la AT-5 (familia Awareness and Training): această politică se aliniază cu AT-1 (Politică și proceduri), AT-2 (Instruire de conștientizare), AT-3 (Instruire bazată pe roluri), AT-4 (Evidențe de instruire în domeniul securității) și AT-5 (Contact cu grupurile de securitate).

11.3.2 IA-5, AC-2: consolidează responsabilitatea utilizatorului privind autentificarea securizată și utilizarea acceptabilă, esențiale pentru rezultatele comportamentale ale programelor de conștientizare.

11.3.3 IR-1 până la IR-8: pregătirea pentru răspunsul la incidente este consolidată prin campanii de conștientizare specifice și simulări.

**11.4 GDPR al UE (2016/679)**

11.4.1 Articolul 32 – Securitatea prelucrării: impune ca personalul care prelucrează date cu caracter personal să fie instruit pentru a recunoaște, preveni și raporta riscurile la adresa datelor cu caracter personal. Această politică asigură instruirea corespunzătoare a persoanelor care prelucrează date cu caracter personal și a tuturor rolurilor relevante.

11.4.2 Articolul 39 – Sarcinile responsabilului cu protecția datelor: include creșterea nivelului de conștientizare și instruirea personalului implicat în operațiunile de prelucrare.

11.4.3 Considerentul 78: încurajează măsuri adecvate de conștientizare pentru a asigura practici de securitate solide și respectarea politicilor.

**11.5 Directiva NIS2 a UE (2022/2555)**

11.5.1 Articolul 21(2)(a, b): impune entităților să adopte politici privind analiza riscurilor și instruirea de securitate pentru întregul personal relevant. Această politică îndeplinește această cerință prin instituirea unor procese continue de instruire, adaptate rolurilor.

11.5.2 Articolul 21(3): încurajează promovarea conștientizării riscurilor de securitate cibernetică în rândul managementului și al personalului prin inițiative de conștientizare și simulări.

**11.6 Regulamentul DORA al UE (2022/2554)**

11.6.1 Articolul 13 – Strategia de reziliență operațională digitală: impune ca nivelul de conștientizare privind riscurile TIC și instruirea să facă parte din modelul de guvernanță. Această politică asigură tratarea riscului uman prin educație continuă și simularea amenințărilor.

11.6.2 Articolele 5 și 8: subliniază importanța unui cadru de control intern, din care conștientizarea și instruirea reprezintă componente fundamentale pentru reziliența TIC și igiena cibernetică.

**11.7 COBIT 2019**

11.7.1 APO07 Gestionarea resurselor umane: consolidează necesitatea dezvoltării conștientizării responsabilităților de securitate și a integrării acestora în managementul forței de muncă.

11.7.2 DSS05 – Managed Security Services: stabilește controale privind instruirea utilizatorilor și raportarea incidentelor, ambele fiind parte integrantă a acestei politici.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: solicită revizuirea eficacității comportamentului utilizatorilor și a respectării politicilor, implementată aici prin teste de phishing, evaluări și indicatori ai campaniilor de conștientizare.