					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P36					Titlul documentului: **Politica privind rețelele sociale și comunicările externe**							
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	Procese definite și guvernanță bazată pe roluri pentru gestionarea comunicărilor publice, asigurând acuratețea, fluxurile de aprobare și escaladarea incidentelor.
ISO/IEC 27002:2022	Controalele 5.10, 5.11, 5.35, 5.36	Reglementează utilizarea informațiilor, utilizarea acceptabilă și comunicarea externă/cu autoritățile, precum și raportarea conformității.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Reguli privind utilizarea sistemelor și comunicațiilor, notificări către utilizatori, păstrarea înregistrărilor de audit.
GDPR al UE	Articolele 5, 25, 32, 33	Principii privind prelucrarea datelor, protecția datelor încă din faza de proiectare, securitatea prelucrării, obligații de notificare a încălcărilor.
Directiva NIS2 a UE	Articolul 21	Măsuri de management al riscurilor de securitate cibernetică, obligații privind incidentele și mesajele publice legate de risc.
Regulamentul DORA al UE	Articolele 9, 16	Managementul riscurilor TIC și strategie de comunicare pentru furnizorii critici.
COBIT 2019	APO09, DSS05	Guvernanța acordurilor de servicii și a comunicării, precum și practici de comunicare securizată/gestionare a incidentelor.

1. Scop

1.1 Prezenta politică stabilește reguli și responsabilități obligatorii care guvernează utilizarea rețelelor sociale și toate formele de comunicare externă de către personalul afiliat organizației.

1.2 Aceasta asigură că mesajele publice — planificate sau spontane — sunt exacte, respectuoase, securizate, conforme din punct de vedere legal și aliniate cu identitatea de brand.

1.3 Politica are ca obiectiv reducerea la minimum a riscurilor asociate prejudiciilor reputaționale, încălcării cerințelor de reglementare, scurgerii de proprietate intelectuală și divulgărilor neautorizate prin canale expuse public.

1.4 De asemenea, politica promovează asumarea responsabilității și o guvernanță structurată în toate formele de comunicare digitală care implică organizația sau o afectează.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor angajaților, contractorilor, stagiarilor și reprezentanților terților care:

2.1.1 Comunică în numele organizației, oficial sau neoficial

2.1.2 Fac referire la organizație sau sugerează afilierea cu aceasta într-un context public

2.1.3 Utilizează conturi personale sau corporative pentru a participa la discuții publice care implică organizația

2.2 Canalele de comunicare vizate includ, fără a se limita la:

2.2.1 Platforme de social media (de exemplu, LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Bloguri, wiki-uri, forumuri și panouri publice de discuții

2.2.3 E-mail sau mesagerie directă către părți externe (de exemplu, clienți, autorități de reglementare, mass-media)

2.2.4 Interviuri de presă, participări la paneluri de discuții sau apariții în materiale media înregistrate

2.2.5 Participarea în comunități online în care organizația este menționată

2.3 Prezenta politică reglementează atât conținutul în timp real, cât și conținutul programat în avans și se aplică tuturor dispozitivelor și conturilor (personale sau corporative) utilizate pentru a difuza comunicarea.

3. Obiective

3.1 Prevenirea divulgării accidentale sau intenționate a informațiilor confidențiale, sensibile sau reglementate prin canale de comunicare externă.

3.2 Asigurarea faptului că declarațiile publice oficiale și conținutul din social media sunt exacte, autorizate și aliniate cu identitatea de brand, etica și mesajele strategice ale organizației.

3.3 Prevenirea prejudiciilor reputaționale și asigurarea consecvenței mesajelor între departamentele interne și platformele externe.

3.4 Respectarea obligațiilor legale aplicabile referitoare la declarațiile publice, inclusiv, dar fără a se limita la, GDPR, NIS2, DORA și normele sectoriale privind comunicările.

3.5 Definirea clară a responsabilităților, a cazurilor de utilizare permise și a protocoalelor de aplicare pentru întregul personal implicat în activități expuse public.

4. Roluri și responsabilități

4.1 Directorul de marketing sau comunicare / responsabilul PR

4.1.1 Aprobă toate mesajele oficiale ale companiei pentru publicare externă

4.1.2 Menține calendarele de conținut pentru rețelele sociale și ghidurile pentru consecvența identității de brand

4.1.3 Monitorizează mențiunile online și expunerea media care implică organizația

4.2 Directorul de securitate a informațiilor (CISO) / echipa de securitate

4.2.1 Monitorizează platformele digitale pentru indicatori de scurgere de date, uzurpare a identității sau tentative de tip phishing

4.2.2 Coordonează cu echipele de răspuns la incidente în cazul atacurilor sau încălcărilor bazate pe platforme sociale

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Aplicare și conformitate

9.1 Prezenta politică este obligatorie pentru întregul personal vizat și pentru terți. Nerespectarea acesteia poate conduce la:

9.1.1 avertismente formale

9.1.2 revocarea temporară sau permanentă a accesului la platforme sau sisteme

9.1.3 măsuri disciplinare, inclusiv încetarea raporturilor de muncă sau contractuale

9.1.4 acțiuni în justiție, dacă comunicarea externă generează prejudicii reputaționale, încălcarea securității datelor sau neconformitate cu reglementările

9.2 Măsuri disciplinare

9.2.1 Încălcările interne (de exemplu, scurgerea datelor confidențiale, defăimarea organizației) vor declanșa implicarea Resurselor Umane, o investigație formală și documentarea în dosarul angajatului.

9.2.2 Acolo unde este aplicabil, funcția juridică va urmări remedii civile sau va notifica autoritățile cu privire la activități infracționale (de exemplu, uzurparea identității, scurgeri legate de tranzacții pe baza informațiilor privilegiate).

9.3 Monitorizarea conformității

9.3.1 Echipele de securitate și de comunicare trebuie să efectueze monitorizarea continuă a:

9.3.1.1 mențiunilor brandului pe principalele platforme

9.3.1.2 utilizării neoficiale a imaginilor companiei sau a mărcilor comerciale

9.3.1.3 riscurilor cunoscute (de exemplu, angajați nemulțumiți, tentative de uzurpare a identității)

9.3.2 Monitorizarea trebuie să respecte legislația și reglementările privind confidențialitatea angajaților, iar toate cazurile semnalate trebuie verificate de un evaluator uman.

9.4 Mecanism de avertizare de integritate și raportarea utilizării abuzive

9.4.1 Orice angajat care suspectează o încălcare a acestei politici este încurajat să o raporteze echipei de securitate a informațiilor, funcției juridice sau anonim, prin portalul de avertizare de integritate.

9.4.2 Orice represalii împotriva persoanelor care raportează nereguli sunt strict interzise și vor face obiectul unor măsuri disciplinare imediate.

10. Cerințe de revizuire și actualizare

10.1 Prezenta politică trebuie revizuită anual sau mai devreme dacă:

10.1.1 Există modificări semnificative ale cerințelor de reglementare (de exemplu, noi acte normative ale UE privind comunicațiile digitale)

10.1.2 Sunt adoptate noi platforme sociale sau noi canale de comunicare

10.1.3 Are loc un incident semnificativ sau apar încălcări repetate care indică lacune de proces

10.1.4 Are loc o schimbare structurală sau de conducere în funcțiile de PR, juridic sau securitate

10.2 Revizuirea trebuie efectuată în comun de către:

10.2.1 Responsabilul de marketing / PR

10.2.2 CISO sau responsabilul pentru riscul de securitate

10.2.3 Responsabilii juridici și de conformitate

10.3 Actualizările trebuie documentate în registrul modificărilor de politică și comunicate prin canale interne de conștientizare. În cazul unor modificări semnificative, întregul personal afectat trebuie să reconfirme luarea la cunoștință a politicii.

11. Politici conexe și interdependențe

11.1 Prezenta politică este susținută de și corelată cu următoarele componente ale Sistemului de management al securității informației (SMSI) al organizației:

11.1.1 P1 – Politica de securitate a informației: stabilește principiile generale pentru protejarea informațiilor, inclusiv asigurarea faptului că comunicările nu conduc la divulgări neautorizate.

11.1.2 P3 – Politica de utilizare acceptabilă: definește comportamentele acceptabile pentru platformele și tehnologiile digitale, care reglementează direct utilizarea personală și profesională a canalelor sociale.

11.1.3 P6 – Politica de management al riscurilor: furnizează cadrul de risc pentru evaluarea amenințărilor legate de comunicarea publică și expunerea reputațională.

11.1.4 P8 – Politica privind conștientizarea și instruirea în domeniul securității informației: stabilește obligații privind programele de conștientizare care instruiesc personalul cu privire la practicile de comunicare securizată și la amenințările de inginerie socială.

11.1.5 P13 – Politica de clasificare și etichetare a datelor: oferă îndrumări personalului privind ceea ce constituie informații restricționate sau confidențiale, care nu trebuie divulgate extern.

11.1.6 P30 – Politica de răspuns la incidente: definește modul de gestionare a incidentelor legate de comunicarea publică, inclusiv scurgerile de date, uzurparea identității și încălcarea cerințelor de reglementare.

11.1.7 P33 – Politica de audit și monitorizare a conformității: reglementează procesele de audit care validează controalele privind social media, sistemele de monitorizare și conformitatea cu politicile de comunicare externă.

12. Standarde și cadre de referință

12.1 ISO/IEC 27001:

12.1.1 Clauza 8.1 – Planificare și control operațional: impune procese definite și guvernanță bazată pe roluri pentru gestionarea comunicărilor publice, asigurând acuratețea, fluxurile de aprobare și escaladarea incidentelor care implică date sau risc reputațional.

12.2 ISO/IEC 27002:2022:

12.2.1 Controlul 5.10 – Utilizarea informațiilor: reglementează diseminarea autorizată și etică a comunicărilor interne sau externe.

12.2.2 Controlul 5.11 – Utilizarea acceptabilă a informațiilor și activelor: consolidează practicile acceptabile pentru distribuirea conținutului utilizând active corporative sau conturi personale.

12.2.3 Controlul 5.35 – Contactul cu autoritățile: impune comunicare externă structurată și autorizată cu autoritățile de reglementare și instituțiile publice.

12.2.4 Controlul 5.36 – Conformitatea cu politicile și standardele: impune aplicarea consecventă a politicilor interne în toate scenariile de comunicare.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Reguli de comportament: impune reguli formale pentru utilizarea sistemelor și comunicațiilor, inclusiv standarde privind divulgarea publică.

12.3.2 AC-8 – Notificare privind utilizarea sistemului: susține clauze de declinare obligatorii și avertizări de conținut pe platformele expuse extern.

12.3.3 AU-12 – Păstrarea înregistrărilor de audit: se aplică păstrării jurnalelor și istoricului comunicațiilor în scopul revizuirii incidentelor și al auditului.

12.4 GDPR al UE (2016/679):

12.4.1 Articolul 5 – Principii privind prelucrarea datelor: interzice distribuirea neautorizată a datelor cu caracter personal prin comunicare publică.

12.4.2 Articolul 25 – Protecția datelor încă din faza de proiectare și în mod implicit: impune măsuri de protecție a confidențialității în instrumentele de comunicare și fluxurile de conținut.

12.4.3 Articolul 32 – Securitatea prelucrării: se aplică criptării, controlului accesului și proceselor de aprobare a conținutului.

12.4.4 Articolul 33 – Notificarea încălcării: impune notificarea în timp util a scurgerilor de date cu caracter personal prin canale publice.

12.5 Directiva NIS2 a UE (2022/2555):

12.5.1 Articolul 21 – Măsuri de management al riscurilor de securitate cibernetică: include protocoale de comunicare și obligații pe durata incidentelor și a mesajelor publice referitoare la risc.

12.6 Regulamentul DORA al UE (2022/2554):

12.6.1 Articolul 9 – Managementul riscurilor TIC: se aplică riscurilor de comunicare declanșate extern, precum uzurparea identității, dezinformarea și perturbarea reputațională.

12.6.2 Articolul 16 – Strategia de comunicare: impune ca furnizorii financiari sau de servicii critici să gestioneze riscurile de comunicare și răspunsurile în scenarii de criză.

12.7 COBIT 2019:

12.7.1 APO09 – Acorduri de servicii gestionate și comunicare: impune guvernanță structurată asupra comunicărilor interne și externe.

12.7.2 DSS05 – Gestionarea serviciilor de securitate: asigură că activitățile de comunicare nu introduc riscuri suplimentare și nu compromit procesele de gestionare a incidentelor.