					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P36S					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	Clauzele 5.1, 5.2, 6.1, 8	Leadership, managementul riscurilor și controlul operațional al comunicărilor externe
ISO/IEC 27002:2022	Controalele 5.10, 5.11	utilizarea acceptabilă a activelor organizației și securitatea informației în comunicare
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Reguli de conduită, audit, raportarea incidentelor și gestionarea conținutului public și a accesului
GDPR al UE	Articolele 5, 32, 33	Principii privind protecția datelor, securitatea prelucrării și notificarea încălcărilor cu impact asupra comunicării publice
Directiva NIS2 a UE	Articolul 21(2)(e), 21(2)(f)	Politici privind utilizarea sistemelor și managementul riscurilor aferente lanțului de aprovizionare și comunicărilor publice
Regulamentul DORA al UE	Articolul 14(4)	Obligații de comunicare ulterioare incidentelor

1. Scop

1.1. Prezenta politică stabilește reguli obligatorii pentru toate comunicările destinate publicului, inclusiv utilizarea rețelelor sociale, interacțiunea cu presa și conținutul digital extern, atunci când se face referire la companie, la personalul acesteia, la clienți, la sisteme sau la practici interne.

1.2. Politica contribuie la protejarea reputației companiei, la menținerea conformității legale și de reglementare și la reducerea riscului de scurgeri de informații, dezinformare sau incidente de securitate.

1.3. Aceasta permite personalului și partenerilor să participe în mod pozitiv și responsabil la discuții online, evitând totodată divulgările accidentale sau prezentările eronate.

1.4. Politica consolidează pregătirea SME pentru certificarea ISO/IEC 27001 prin abordarea controlului informațiilor puse la dispoziția publicului sau a părților interesate externe.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică tuturor persoanelor afiliate organizației, inclusiv:

2.1.1. Angajaților și contractorilor

2.1.2. Freelancerilor, consultanților și furnizorilor terți

2.1.3. Stagiarilor sau personalului cu normă parțială implicat în livrarea către clienți sau cu acces la sisteme

2.2. Politica se aplică tuturor formelor de comunicare externă care fac referire la organizație, inclusiv:

2.2.1. Postărilor pe rețele sociale (LinkedIn, Twitter/X, TikTok, Instagram, Facebook etc.)

2.2.2. Articolelor de blog, forumurilor online, recenziilor clienților și firelor de discuție

2.2.3. Participărilor în calitate de vorbitor la evenimente (de exemplu, conferințe, webinare, podcasturi)

2.2.4. E-mailurilor sau mesajelor adresate jurnaliștilor, reprezentanților autorităților publice sau influencerilor

2.2.5. Capturilor de ecran, fotografiilor sau videoclipurilor distribuite public din mediile de lucru

2.3. Politica se aplică și atunci când astfel de comunicări sunt realizate:

2.3.1. De pe dispozitive sau conturi personale

2.3.2. În afara programului normal de lucru

2.3.3. Fără intenție malițioasă; chiar și remarci accidentale sau făcute în treacăt intră în domeniul de aplicare dacă fac referire la companie

3. Obiective

3.1. Protejarea reputației: prevenirea afectării imaginii companiei prin comunicări publice neautorizate sau necorespunzătoare

3.2. Securitatea datelor: evitarea expunerii neintenționate a datelor sensibile, a sistemelor interne sau a detaliilor despre clienți prin rețele sociale sau canale publice

3.3. Conformitate legală și de reglementare: asigurarea faptului că orice conținut public care face referire la companie respectă legislația aplicabilă privind protecția datelor și comunicările de afaceri

3.4. Conduită profesională: încurajarea participării responsabile la discuții online și a interacțiunilor cu mass-media, inclusiv din conturi personale

3.5. Pregătire pentru incidente: stabilirea unor pași clari și aplicabili în caz de divulgări accidentale sau încălcări ale politicii

4. Roluri și responsabilități

4.1. Directorul general (GM)

4.1.1. Este proprietarul prezentei politici și o aprobă

4.1.2. Revizuiește și autorizează orice declarații destinate publicului, interacțiuni cu presa sau interviuri în mass-media

4.1.3. Se asigură că această politică este comunicată clar tuturor angajaților și terților

4.1.4. Investigă și gestionează orice încălcări ale prezentei politici, în coordonare cu procedurile de răspuns la incidente

4.2. Angajatul desemnat sau responsabilul de comunicare (dacă este desemnat)

4.2.1. Sprijină GM prin revizuirea conținutului înainte de publicarea externă (de exemplu, articole de blog, teme de prezentare)

4.2.2. Menține jurnale ale activităților media aprobate sau ale postărilor din rețelele sociale cu risc ridicat

4.2.3. Monitorizează, în limita capacității disponibile, mențiunile cunoscute ale companiei în mediul online pentru identificarea riscurilor reputaționale sau de securitate

[... 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 cel puțin o dată pe an de către Directorul general (GM)

9.1.2. Revizuirea trebuie să asigure alinierea la obligațiile legale actualizate, la tendințele din comunicarea în industrie și la schimbările interne din activitățile organizației

9.2. Revizuiri declanșate de evenimente

9.2.1. Această politică trebuie actualizată imediat după:

9.2.1.1. Un incident semnificativ pe rețele sociale sau o problemă reputațională

9.2.1.2. O schimbare a furnizorilor terți care gestionează comunicările

9.2.1.3. O nouă legislație sau noi obligații de reglementare privind comunicarea online, mass-media sau identitatea de brand

9.3. Documentarea modificărilor

9.3.1. Toate actualizările trebuie înregistrate, inclusiv data revizuirii, rezumatul modificărilor și aprobarea GM

9.3.2. Trebuie păstrat un istoric al versiunilor în scopuri de audit și certificare

9.4. Distribuirea actualizărilor

9.4.1. Întregul personal și contractorii trebuie informați cu privire la orice modificare a politicii

9.4.2. Versiunile actualizate trebuie distribuite prin e-mail sau prin portaluri interne

9.4.3. Orice furnizor de comunicări publice trebuie să confirme noile condiții înainte de continuarea activității

10. Politici conexe și interdependențe

10.1. Prezenta politică funcționează în coordonare cu următoarele politici SME:

10.1.1. P3S – Politica de utilizare acceptabilă: definește comportamentul acceptabil la utilizarea platformelor de comunicare, inclusiv accesul la rețele sociale în timpul programului de lucru

10.1.2. P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: asigură instruirea personalului pentru identificarea riscurilor de divulgare excesivă, a atacurilor de tip phishing sau a amenințărilor reputaționale online

10.1.3. P17S – Politica de protecție a datelor și confidențialitate: asigură că datele cu caracter personal și datele clienților nu sunt distribuite în comunicări externe, în conformitate cu GDPR și alte cerințe legale

10.1.4. P30S – Politica de răspuns la incidente: reglementează răspunsul la divulgarea publică accidentală, amenințările online sau atacurile reputaționale rezultate din utilizarea necorespunzătoare a rețelelor sociale

10.1.5. P37S – Politica de conformitate legală și de reglementare: stabilește obligațiile legale și contractuale generale ale organizației atunci când distribuie conținut în mod public

10.2. Aceste politici trebuie aplicate împreună pentru a menține o prezență externă sigură, respectuoasă și conformă din punct de vedere legal.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 5.1 – Leadership și angajament: impune supravegherea de către conducere a riscurilor reputaționale și a riscurilor privind informațiile

11.1.2. Clauza 6.1 – Managementul riscurilor: include expunerile la risc aferente comunicării

11.1.3. Clauza 8.1 – Control operațional: acoperă regulile privind modul în care informațiile sunt comunicate în exterior

11.2. ISO/IEC 27002

11.2.1. Controlul 5.10 – Utilizarea acceptabilă a activelor organizației și a informațiilor

11.2.2. Controlul 5.11 – Securitatea informației în comunicare

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Reguli de conduită: reglementează conduita adecvată privind utilizarea resurselor informaționale

11.3.2. AU-7 – Reducerea auditului și generarea de rapoarte: sprijină monitorizarea utilizării sistemelor publice

11.3.3. IR-6 – Raportarea incidentelor: impune răspunsul la încălcări reputaționale și de comunicare

11.3.4. AC-22 – Conținut accesibil publicului: asigură controlul asupra publicațiilor externe și accesului

11.4. GDPR al UE (2016/679)

11.4.1. Articolul 5 – Principii privind prelucrarea datelor cu caracter personal (exactitate, integritate, responsabilitate)

11.4.2. Articolul 32 – Securitatea prelucrării: impune măsuri de protecție pentru distribuirea publică

11.4.3. Articolul 33 – Notificarea încălcărilor: se aplică atunci când datele cu caracter personal sunt expuse prin comunicare externă

11.5. Directiva NIS2 a UE (2022/2555)

11.5.1. Articolul 21(2)(e) – Politici privind utilizarea sistemelor informatice, inclusiv a platformelor de comunicare

11.5.2. Articolul 21(2)(f) – Politici pentru gestionarea riscurilor de securitate cibernetică în lanțul de aprovizionare și pe platformele publice

11.6. Regulamentul DORA al UE (2022/2554)

11.6.1. Articolul 14(4) – Obligații de comunicare către clienți, terți și autorități în urma incidentelor operaționale

11.7. COBIT 2019

11.7.1. APO09 – Manage Service Agreements: acoperă supravegherea furnizorilor și a terților implicați în comunicare

11.7.2. DSS05 – Manage Security Services: include protejarea activelor digitale destinate publicului

11.7.3. EDM03 – Ensure Risk Optimization: evidențiază gestionarea riscurilor reputaționale și de conformitate legate de comunicare