					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P36S					Názov dokumentu: **Politika sociálnych médií a externej komunikácie**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Články 5.1, 5.2, 6.1, 8	Vedenie, riziká a prevádzkové opatrenia externej komunikácie
ISO/IEC 27002:2022	Opatrenia 5.10, 5.11	prijateľné používanie podnikových aktív a informačná bezpečnosť v komunikácii
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	pravidlá správania, audit, nahlasovanie incidentov a riadenie verejne prístupného obsahu a prístupu
GDPR EÚ	Články 5, 32, 33	zásady ochrany osobných údajov, bezpečnosť a oznamovanie porušenia ochrany osobných údajov ovplyvňujúce verejnú komunikáciu
NIS2 EÚ	Článok 21(2)(e), 21(2)(f)	politiky používania systémov a riadenie rizík dodávateľského reťazca/verejnej komunikácie
DORA EÚ	Článok 14(4)	komunikačné povinnosti po incidentoch

1. Účel

1.1. Táto politika stanovuje záväzné pravidlá pre všetku verejnú komunikáciu vrátane používania sociálnych médií, komunikácie s médiami a externého digitálneho obsahu, ak sa týka spoločnosti, jej zamestnancov, klientov, systémov alebo interných postupov.

1.2. Politika pomáha chrániť reputáciu spoločnosti, udržiavať súlad so zákonnými a regulačnými požiadavkami a znižovať riziko úniku informácií, dezinformácií alebo bezpečnostných incidentov.

1.3. Umožňuje zamestnancom a partnerom zapájať sa do online diskusií pozitívne a zodpovedne a zároveň predchádzať náhodnému zverejneniu informácií alebo nesprávnej prezentácii.

1.4. Politika posilňuje pripravenosť MSP na certifikáciu podľa ISO/IEC 27001 tým, že upravuje riadenie informácií sprístupňovaných verejnosti alebo externým zainteresovaným stranám.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky osoby prepojené s organizáciou vrátane:

2.1.1. zamestnancov a zmluvných pracovníkov,

2.1.2. freelancerov, konzultantov a dodávateľov tretích strán,

2.1.3. stážistov alebo pracovníkov na čiastočný úväzok zapojených do poskytovania služieb klientom alebo s prístupom do systémov.

2.2. Politika sa vzťahuje na všetky formy externej komunikácie, ktoré sa týkajú organizácie, vrátane:

2.2.1. príspevkov na sociálnych médiách (LinkedIn, Twitter/X, TikTok, Instagram, Facebook a pod.),

2.2.2. blogových príspevkov, online fór, zákazníckych recenzií a diskusných vlákien,

2.2.3. verejných vystúpení (napr. konferencie, webináre, podcasty),

2.2.4. e-mailov alebo správ novinárom, zástupcom orgánov verejnej moci alebo influencerom,

2.2.5. verejne zdieľaných snímok obrazovky, fotografií alebo videí z pracovného prostredia.

2.3. Politika sa uplatňuje aj v prípade, ak je takáto komunikácia uskutočnená:

2.3.1. zo súkromných zariadení alebo účtov,

2.3.2. mimo bežného pracovného času,

2.3.3. bez úmyslu spôsobiť škodu — do rozsahu tejto politiky patria aj náhodné alebo neformálne vyjadrenia, ak sa týkajú spoločnosti.

3. Ciele

3.1. Ochrana reputácie: Predchádzať poškodeniu dobrého mena spoločnosti v dôsledku neautorizovanej alebo nevhodnej verejnej komunikácie.

3.2. Bezpečnosť údajov: Predchádzať neúmyselnému sprístupneniu citlivých údajov, informácií o interných systémoch alebo detailov o klientoch prostredníctvom sociálnych médií alebo verejných kanálov.

3.3. Zákonný a regulačný súlad: Zabezpečiť, aby bol všetok verejný obsah týkajúci sa spoločnosti v súlade s príslušnými právnymi predpismi v oblasti ochrany údajov a obchodnej komunikácie.

3.4. Profesionálne správanie: Podporovať zodpovednú účasť v online diskusiách a komunikácii s médiami, a to aj na osobných účtoch.

3.5. Pripravenosť na incidenty: Poskytnúť jasné a vykonateľné kroky pre prípad náhodného zverejnenia informácií alebo porušenia tejto politiky.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. je vlastníkom tejto politiky a schvaľuje ju,

4.1.2. preskúmava a schvaľuje všetky verejné vyhlásenia, komunikáciu s médiami a mediálne rozhovory,

4.1.3. zabezpečuje, aby bola táto politika jednoznačne komunikovaná všetkým zamestnancom a tretím stranám,

4.1.4. vyšetruje a rieši každé porušenie tejto politiky v koordinácii s postupmi reakcie na incidenty.

4.2. Určený zamestnanec alebo vedúci komunikácie (ak je určený)

4.2.1. podporuje GM pri preskúmaní obsahu pred jeho externým zverejnením (napr. blogové príspevky, témy vystúpení),

4.2.2. vedie záznamy o schválenej mediálnej aktivite alebo vysokorizikových príspevkoch na sociálnych médiách,

4.2.3. v rozsahu dostupných kapacít monitoruje známe zmienky o spoločnosti v online priestore z pohľadu reputačných alebo bezpečnostných rizík.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1. Ročné preskúmanie

9.1.1. Túto politiku musí najmenej raz ročne preskúmať generálny manažér (GM).

9.1.2. Preskúmanie musí zabezpečiť súlad s aktualizovanými zákonnými povinnosťami, trendmi v oblasti komunikácie a internými zmenami v činnosti organizácie.

9.2. Preskúmania vyvolané udalosťou

9.2.1. Táto politika musí byť bezodkladne aktualizovaná po:

9.2.1.1. významnom incidente na sociálnych médiách alebo reputačnom probléme,

9.2.1.2. zmene dodávateľov tretích strán, ktorí riadia komunikáciu,

9.2.1.3. prijatí novej legislatívy alebo vzniku nových regulačných povinností týkajúcich sa online komunikácie, médií alebo značky.

9.3. Dokumentovanie zmien

9.3.1. Každá aktualizácia musí byť zaznamenaná vrátane dátumu revízie, súhrnu zmien a schválenia zo strany GM.

9.3.2. Na účely auditu a certifikácie sa musí uchovávať evidencia verzií.

9.4. Distribúcia aktualizácií

9.4.1. Všetci zamestnanci a zmluvní pracovníci musia byť informovaní o každej zmene politiky.

9.4.2. Aktualizované verzie musia byť distribuované e-mailom alebo prostredníctvom interných portálov.

9.4.3. Každý dodávateľ zabezpečujúci verejnú komunikáciu musí pred pokračovaním v činnosti potvrdiť oboznámenie sa s aktualizovanými podmienkami.

10. Súvisiace politiky a väzby

10.1. Táto politika sa uplatňuje v koordinácii s nasledujúcimi politikami SME:

10.1.1. P3S – Politika prijateľného používania: definuje prípustné správanie pri používaní komunikačných platforiem vrátane prístupu k sociálnym médiám počas pracovného času.

10.1.2. P8S – Politika povedomia a školenia v oblasti informačnej bezpečnosti: zabezpečuje, aby boli zamestnanci vyškolení na rozpoznanie rizík nadmerného zdieľania, phishingu alebo reputačných hrozieb v online priestore.

10.1.3. P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby sa v externej komunikácii nezdieľali osobné údaje ani údaje zákazníkov v súlade s GDPR a ďalšími právnymi požiadavkami.

10.1.4. P30S – Politika reakcie na incidenty: upravuje reakciu na náhodné verejné zverejnenie informácií, online hrozby alebo reputačné útoky vyplývajúce zo zneužitia sociálnych médií.

10.1.5. P37S – Politika zákonného a regulačného súladu: stanovuje širšie zákonné a zmluvné povinnosti organizácie pri verejnom zdieľaní obsahu.

10.2. Tieto politiky sa musia uplatňovať spoločne s cieľom zachovať bezpečnú, profesionálnu a právne súladnú externú prezentáciu organizácie.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Článok 5.1 – Vedenie a záväzok: vyžaduje dohľad vedenia nad reputačnými a informačnými rizikami.

11.1.2. Článok 6.1 – Riadenie rizík: zahŕňa expozíciu rizikám súvisiacim s komunikáciou.

11.1.3. Článok 8.1 – Prevádzkové opatrenia: upravuje pravidlá externej komunikácie informácií.

11.2. ISO/IEC 27002

11.2.1. Opatrenie 5.10 – prijateľné používanie podnikových aktív a informácií

11.2.2. Opatrenie 5.11 – informačná bezpečnosť v komunikácii

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – pravidlá správania: upravujú primerané správanie pri používaní informačných zdrojov.

11.3.2. AU-7 – redukcia auditu a generovanie správ: podporuje monitorovanie používania verejných systémov.

11.3.3. IR-6 – nahlasovanie incidentov: vyžaduje reakciu na reputačné incidenty a porušenia súvisiace s komunikáciou.

11.3.4. AC-22 – verejne prístupný obsah: zabezpečuje riadenie externých publikácií a prístupu.

11.4. GDPR EÚ (2016/679)

11.4.1. Článok 5 – zásady spracúvania osobných údajov (presnosť, integrita, zodpovednosť).

11.4.2. Článok 32 – bezpečnosť spracúvania: vyžaduje ochranné opatrenia pri verejnom zdieľaní.

11.4.3. Článok 33 – oznámenie porušenia ochrany osobných údajov: uplatní sa, ak sú osobné údaje sprístupnené prostredníctvom externej komunikácie.

11.5. Smernica EÚ NIS2 (2022/2555)

11.5.1. Článok 21(2)(e) – politiky používania informačných systémov vrátane komunikačných platforiem.

11.5.2. Článok 21(2)(f) – politiky na riešenie rizík kybernetickej bezpečnosti v dodávateľskom reťazci a na verejných platformách.

11.6. Nariadenie EÚ DORA (2022/2554)

11.6.1. Článok 14(4) – komunikačné povinnosti voči zákazníkom, tretím stranám a orgánom po prevádzkových incidentoch.

11.7. COBIT 2019

11.7.1. APO09 – riadenie servisných dohôd: pokrýva dohľad nad dodávateľmi a tretími stranami súvisiacimi s komunikáciou.

11.7.2. DSS05 – riadenie bezpečnostných služieb: zahŕňa ochranu digitálnych aktív vystavených verejnosti.

11.7.3. EDM03 – zabezpečenie optimalizácie rizík: zdôrazňuje riadenie reputačných rizík a rizík súladu súvisiacich s komunikáciou.