| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem zadajte názov registrovanej právnickej osoby | | | | | | | |
| Číslo dokumentu:<br>P36 | | | | | Názov dokumentu:<br>**Politika sociálnych médií a externej komunikácie** | | | | | | | |
| Verzia:<br>1.0 | | Dátum nadobudnutia účinnosti:<br>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** |
| | | | |
| | | | |

Zosúladenie s normami a predpismi

| Norma/predpis | Kapitola/článok | Poznámka |
|---|---|---|
| ISO/IEC 27001:2022 | Kapitola 8 | Definované procesy a riadenie založené na roliach pri riadení verejnej komunikácie, zabezpečení presnosti, schvaľovacích workflowoch a eskalácii incidentov. |
| ISO/IEC 27002:2022 | Kontroly 5.10, 5.11, 5.35, 5.36 | Upravuje používanie informácií, prijateľné používanie podnikových aktív, komunikáciu s externými kontaktmi a orgánmi a preukazovanie súladu. |
| NIST SP 800-53 Rev.5 | AC-8, AU-12, PL-4 | Pravidlá používania systémov a komunikácie, upozornenia používateľom a uchovávanie auditných záznamov. |
| GDPR EÚ | Články 5, 25, 32, 33 | Zásady spracúvania osobných údajov, ochrana súkromia už pri návrhu a štandardne, bezpečnosť spracúvania a povinnosti oznamovania porušenia ochrany osobných údajov. |
| Smernica EÚ NIS2 | Článok 21 | Opatrenia riadenia rizík kybernetickej bezpečnosti, povinnosti pri incidentoch a verejnej komunikácii súvisiacej s rizikami. |
| Nariadenie EÚ DORA | Články 9, 16 | Riadenie IKT rizík a komunikačná stratégia pre kritických poskytovateľov. |
| COBIT 2019 | APO09, DSS05 | Riadenie servisných dohôd a komunikácie a bezpečné komunikačné postupy a riadenie incidentov. |

Účel

1.1 Táto politika stanovuje záväzné pravidlá a zodpovednosti pre používanie sociálnych médií a všetkých foriem externej komunikácie osobami pridruženými k organizácii.

1.2 Zabezpečuje, aby verejná komunikácia, či už plánovaná alebo spontánna, bola presná, rešpektujúca, bezpečná, v súlade s právnymi požiadavkami a konzistentná so značkou organizácie.

1.3 Cieľom politiky je minimalizovať riziká súvisiace s reputačnou ujmou, porušením regulačných požiadaviek, únikom duševného vlastníctva a neoprávneným zverejnením informácií prostredníctvom verejne prístupných systémov.

1.4 Politika ďalej podporuje preukázateľnú zodpovednosť a štruktúrované riadenie vo všetkých formách digitálnej komunikácie, ktorá sa týka organizácie alebo ju ovplyvňuje.

**2. Rozsah**

**2.1 Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných pracovníkov, stážistov a zástupcov tretích strán, ktorí:**

2.1.1 komunikujú v mene organizácie, či už oficiálne alebo neformálne,

2.1.2 odkazujú na svoju príslušnosť k organizácii alebo ju naznačujú vo verejnom priestore,

2.1.3 používajú osobné alebo podnikové účty na zapájanie sa do verejných diskusií týkajúcich sa organizácie.

**2.2 Medzi komunikačné kanály zahrnuté do rozsahu patria okrem iného:**

2.2.1 platformy sociálnych médií (napr. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook),

2.2.2 blogy, wiki, fóra a verejné diskusné platformy,

2.2.3 e-mail alebo priame správy externým stranám (napr. klientom, regulačným orgánom, médiám),

2.2.4 tlačové rozhovory, diskusné panely alebo zaznamenané mediálne vystúpenia,

2.2.5 účasť v online komunitách, v ktorých sa spomína organizácia.

2.3 Táto politika upravuje obsah v reálnom čase aj vopred naplánovaný obsah a vzťahuje sa na všetky zariadenia a účty (osobné aj podnikové) používané na šírenie komunikácie.

**3. Ciele**

3.1 Predchádzať náhodnému alebo úmyselnému zverejneniu dôverných, citlivých alebo regulovaných informácií prostredníctvom kanálov externej komunikácie.

3.2 Zabezpečiť, aby oficiálne verejné vyhlásenia a obsah na sociálnych médiách boli presné, autorizované a v súlade s firemnou identitou, etikou a strategickou komunikáciou.

3.3 Predchádzať reputačnej ujme a zabezpečiť konzistentnosť komunikácie naprieč internými oddeleniami a externými platformami.

3.4 Dodržiavať príslušné zákonné povinnosti súvisiace s verejnými vyhláseniami vrátane GDPR, NIS2, DORA a pravidiel komunikácie špecifických pre dané odvetvie.

3.5 Vymedziť jasné zodpovednosti, prijateľné spôsoby používania a postupy presadzovania politiky pre všetkých pracovníkov zapojených do aktivít vystavených verejnosti.

**4. Roly a zodpovednosti**

**4.1 Riaditeľ marketingu alebo komunikácie / vedúci PR**

4.1.1 schvaľuje všetku oficiálnu komunikáciu spoločnosti určenú na externé zverejnenie,

4.1.2 riadi harmonogramy obsahu sociálnych médií a usmernenia na zabezpečenie konzistentnosti značky,

4.1.3 monitoruje online zmienky a mediálne výstupy týkajúce sa organizácie.

**4.2 Riaditeľ informačnej bezpečnosti (CISO) / tím informačnej bezpečnosti**

4.2.1 monitoruje digitálne platformy s cieľom identifikovať indikátory únikov údajov, vydávania sa za inú osobu alebo pokusov o phishing,

4.2.2 koordinuje postup s tímami reakcie na incidenty v prípade útokov alebo porušení súvisiacich so sociálnymi médiami.

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

**9. Presadzovanie politiky a súlad**

**9.1 Táto politika je záväzná pre všetkých dotknutých pracovníkov a tretie strany. Nedodržanie môže viesť k:**

9.1.1 formálnym upozorneniam,

9.1.2 dočasnému alebo trvalému odobraniu prístupu k platformám alebo systémom,

9.1.3 disciplinárnym opatreniam vrátane ukončenia pracovného pomeru alebo spolupráce,

9.1.4 súdnemu alebo inému právnemu konaniu, ak externá komunikácia vedie k reputačnej ujme, porušeniu ochrany osobných údajov alebo regulačnému nesúladu.

**9.2 Disciplinárne opatrenia**

9.2.1 Interné porušenia (napr. únik dôverných údajov, poškodzovanie dobrého mena organizácie) vedú k zapojeniu HR, formálnemu vyšetrovaniu a zdokumentovaniu v osobnom spise zamestnanca.

9.2.2 Ak je to relevantné, právne oddelenie uplatní občianskoprávne prostriedky nápravy alebo oznámi orgánom činným v trestnom konaní podozrenie na trestnú činnosť (napr. vydávanie sa za inú osobu, úniky informácií súvisiace s insider tradingom).

**9.3 Monitorovanie súladu**

**9.3.1 Bezpečnostný a komunikačný tím musia vykonávať priebežné monitorovanie:**

9.3.1.1 zmienok o značke na hlavných platformách,

9.3.1.2 neoficiálneho používania obrazových materiálov spoločnosti alebo ochranných známok,

9.3.1.3 známych rizík (napr. nespokojní zamestnanci, pokusy o vydávanie sa za inú osobu).

9.3.2 Monitorovanie musí byť v súlade s právnymi predpismi na ochranu súkromia zamestnancov a všetky označené prípady musia byť overené človekom.

**9.4 Oznamovanie porušení a zneužitia**

9.4.1 Každý zamestnanec, ktorý má podozrenie na porušenie tejto politiky, má povinnosť nahlásiť ho tímu informačnej bezpečnosti, právnemu oddeleniu alebo anonymne prostredníctvom mechanizmu oznamovania porušení.

9.4.2 Odvetné opatrenia voči oznamovateľom sú prísne zakázané a budú predmetom okamžitých disciplinárnych opatrení.

## 10. Požiadavky na preskúmanie a aktualizáciu

**10.1 Táto politika sa musí preskúmať najmenej raz ročne alebo skôr, ak:**

10.1.1 dôjde k významným zmenám regulačných požiadaviek (napr. nové právne predpisy EÚ v oblasti digitálnej komunikácie),

10.1.2 sa zavedú nové sociálne platformy alebo komunikačné kanály,

10.1.3 dôjde k významnému incidentu alebo opakovaným porušeniam, ktoré naznačujú medzery v procesoch,

10.1.4 dôjde k organizačnej alebo personálnej zmene vo funkciách PR, právnych záležitostí alebo bezpečnosti.

**10.2 Preskúmanie musia spoločne vykonať:**

10.2.1 vedúci marketingu / PR,

10.2.2 CISO alebo vedúci bezpečnostných rizík,

10.2.3 pracovníci právnej a compliance funkcie.

10.3 Aktualizácie musia byť zdokumentované v registri zmien politík a komunikované prostredníctvom interných kanálov zvyšovania povedomia. Ak dôjde k podstatným zmenám, všetci dotknutí pracovníci musia opätovne potvrdiť oboznámenie sa s politikou.

## 11. Súvisiace politiky a väzby

**11.1 Táto politika je podporená a vzájomne prepojená s nasledujúcimi súčasťami systému manažérstva informačnej bezpečnosti (ISMS) organizácie:**

11.1.1 P1 – Politika informačnej bezpečnosti: stanovuje nadradené zásady ochrany informácií vrátane zabezpečenia, aby komunikácia neviedla k neoprávnenému zverejneniu.

11.1.2 P3 – Politika prijateľného používania: vymedzuje prijateľné správanie pri používaní digitálnych platforiem a technológií, ktoré priamo upravuje osobné aj profesionálne používanie sociálnych kanálov.

11.1.3 P6 – Politika riadenia rizík: poskytuje rámec riadenia rizík na posudzovanie hrozieb súvisiacich s verejnou komunikáciou a reputačnou expozíciou.

11.1.4 P8 – Politika povedomia a školenia o informačnej bezpečnosti: stanovuje programy zvyšovania povedomia, ktoré vzdelávajú pracovníkov v oblasti bezpečných komunikačných postupov a hrozieb sociálneho inžinierstva.

11.1.5 P13 – Politika klasifikácie a označovania údajov: usmerňuje pracovníkov v tom, čo predstavuje obmedzené alebo dôverné informácie, ktoré nesmú byť zverejnené externe.

11.1.6 P30 – Politika reakcie na incidenty: vymedzuje spôsob riešenia incidentov súvisiacich s verejnou komunikáciou vrátane únikov údajov, vydávania sa za inú osobu a regulačného nesúladu.

11.1.7 P33 – Politika monitorovania auditu a súladu: upravuje auditné procesy, ktoré overujú kontroly sociálnych médií, monitorovacie systémy a súlad s politikami externej komunikácie.

## 12. Referenčné normy a rámce

### 12.1 ISO/IEC 27001:

12.1.1 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: vyžaduje definované procesy a riadenie založené na roliach pri riadení verejnej komunikácie, zabezpečení presnosti, schvaľovacích workflowoch a eskalácii incidentov zahŕňajúcich riziko pre údaje alebo reputáciu.

### 12.2 ISO/IEC 27002:2022:

12.2.1 Kontrola 5.10 – Používanie informácií: upravuje autorizované a etické šírenie internej alebo externej komunikácie.

12.2.2 Kontrola 5.11 – Prijateľné používanie podnikových aktív: posilňuje prijateľné postupy pri zdieľaní obsahu prostredníctvom podnikových aktív alebo osobných účtov.

12.2.3 Kontrola 5.35 – Kontakt s orgánmi: vyžaduje štruktúrovanú a autorizovanú externú komunikáciu s regulačnými orgánmi a verejnými inštitúciami.

12.2.4 Kontrola 5.36 – Súlad s politikami a normami: vyžaduje konzistentné uplatňovanie interných politík vo všetkých scenároch komunikácie.

### 12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Pravidlá správania: vyžaduje formálne pravidlá používania systémov a komunikácie vrátane štandardov verejného zverejňovania.

12.3.2 AC-8 – Upozornenie na používanie systému: podporuje povinné vyhlásenia o vylúčení zodpovednosti a upozornenia na obsah na externe vystavených platformách.

12.3.3 AU-12 – Uchovávanie auditných záznamov: vzťahuje sa na uchovávanie logov a histórie komunikácie na účely preskúmania incidentov a auditu.

### 12.4 Nariadenie EÚ GDPR (2016/679):

12.4.1 Článok 5 – Zásady spracúvania osobných údajov: zakazuje neoprávnené zdieľanie osobných údajov prostredníctvom verejnej komunikácie.

12.4.2 Článok 25 – Ochrana súkromia už pri návrhu a štandardne: vyžaduje opatrenia na ochranu súkromia v komunikačných nástrojoch a workflowoch obsahu.

12.4.3 Článok 32 – Bezpečnosť spracúvania: uplatňuje šifrovanie, riadenie prístupu a procesy schvaľovania obsahu.

12.4.4 Článok 33 – Oznámenie porušenia ochrany osobných údajov: stanovuje povinnosť včasného oznámenia únikov osobných údajov prostredníctvom verejných kanálov.

**12.5 Smernica EÚ NIS2 (2022/2555):**

12.5.1 Článok 21 – Opatrenia riadenia rizík kybernetickej bezpečnosti: zahŕňa komunikačné protokoly a povinnosti počas incidentov a verejnej komunikácie o rizikách.

**12.6 Nariadenie EÚ DORA (2022/2554):**

12.6.1 Článok 9 – Riadenie IKT rizík: vzťahuje sa na externe vyvolané komunikačné riziká, ako sú vydávanie sa za inú osobu, dezinformácie a reputačné narušenie.

12.6.2 Článok 16 – Komunikačná stratégia: vyžaduje, aby kritickí finanční alebo servisní poskytovatelia riadili komunikačné riziká a reakcie v krízových situáciách.

**12.7 COBIT 2019:**

12.7.1 APO09 – Riadené servisné dohody a komunikácia: vyžaduje štruktúrované riadenie internej a externej komunikácie.

12.7.2 DSS05 – Riadenie bezpečnostných služieb: zabezpečuje, aby komunikačné aktivity nevnášali dodatočné riziko ani nenarúšali procesy riešenia incidentov.