					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P36S					Naslov dokumenta: **Politika družbenih medijev in zunanjega komuniciranja**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	Opredeljeni procesi in upravljanje na podlagi vlog za upravljanje javnega komuniciranja, ki zagotavljajo točnost, odobritvene poteke dela in eskalacijo incidentov.
ISO/IEC 27002:2022	Kontrole 5.10, 5.11, 5.35, 5.36	Ureja uporabo, sprejemljivo uporabo ter zunanje komuniciranje s pristojnimi organi in poročanje o skladnosti.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Pravila uporabe sistemov in komunikacij, obvestila uporabnikom ter hrambo revizijskih zapisov.
Uredba EU GDPR	Členi 5, 25, 32, 33	Načela obdelave osebnih podatkov, varstvo podatkov že pri načrtovanju, varnost obdelave in zahteve glede obveščanja o kršitvah.
Direktiva EU NIS2	Člen 21	Ukrepi za upravljanje tveganj kibernetske varnosti ter obveznosti v primeru incidentov in javnega komuniciranja, povezanega s tveganji.
Uredba EU DORA	Členi 9, 16	Upravljanje tveganj IKT in komunikacijska strategija za kritične ponudnike.
COBIT 2019	APO09, DSS05	Upravljanje sporazumov o storitvah in komuniciranja ter varne komunikacijske prakse in upravljanje incidentov.

1. Namen

1.1 Ta politika določa obvezna pravila in odgovornosti za uporabo družbenih medijev ter vseh oblik zunanjega komuniciranja s strani osebja, povezanega z organizacijo.

1.2 Zagotavlja, da so javna sporočila – načrtovana ali spontana – točna, spoštljiva, varna, skladna s pravnimi zahtevami in usklajena z blagovno znamko organizacije.

1.3 Namen te politike je zmanjšati tveganja, povezana s škodo za ugled, regulativnimi kršitvami, razkritjem intelektualne lastnine in nepooblaščenimi razkritji prek javno dostopnih kanalov.

1.4 Ta politika dodatno spodbuja odgovornost in strukturirano upravljanje vseh oblik digitalnega komuniciranja, ki vključujejo organizacijo ali vplivajo nanjo.

2. Področje uporabe

2.1 Ta politika velja za vse zaposlene, pogodbene izvajalce, praktikante in predstavnike tretjih oseb, ki:

2.1.1 komunicirajo v imenu organizacije, uradno ali neuradno,

2.1.2 se v javnem okolju sklicujejo na povezanost z organizacijo ali jo nakazujejo,

2.1.3 uporabljajo osebne ali korporativne račune za sodelovanje v javnih razpravah, povezanih z organizacijo.

2.2 Komunikacijski kanali, zajeti s to politiko, med drugim vključujejo:

2.2.1 platforme družbenih medijev (npr. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook),

2.2.2 bloge, wikije, forume in javne razpravljalne table,

2.2.3 e-pošto ali neposredno sporočanje zunanjim deležnikom (npr. strankam, regulatorjem, medijem),

2.2.4 intervjuje za medije, panelne razprave ali nastope v posnetih medijskih vsebinah,

2.2.5 sodelovanje v spletnih skupnostih, v katerih se omenja organizacija.

2.3 Ta politika ureja vsebine v realnem času in vnaprej načrtovane vsebine ter velja za vse naprave in račune (osebne ali korporativne), ki se uporabljajo za razširjanje komunikacije.

3. Cilji

3.1 Preprečiti nenamerno ali namerno razkritje zaupnih, občutljivih ali reguliranih informacij prek kanalov zunanjega komuniciranja.

3.2 Zagotoviti, da so uradne javne izjave in vsebine na družbenih medijih točne, odobrene in usklajene s korporativno identiteto, etičnimi načeli in strateškimi sporočili.

3.3 Preprečiti škodo za ugled in zagotoviti doslednost sporočanja med notranjimi oddelki in zunanjimi platformami.

3.4 Izpolnjevati veljavne pravne obveznosti, povezane z javnimi izjavami, vključno z GDPR, NIS2, DORA in sektorskimi pravili komuniciranja.

3.5 Opredeliti jasne odgovornosti, dopustne primere uporabe in protokole izvajanja za vse osebje, vključeno v javno izpostavljene dejavnosti.

4. Vloge in odgovornosti

4.1 direktor marketinga ali komuniciranja / vodja odnosov z javnostmi

4.1.1 odobrava vsa uradna sporočila organizacije za zunanjo objavo,

4.1.2 vzdržuje uredniški koledar za družbene medije in smernice za dosledno uporabo blagovne znamke,

4.1.3 spremlja spletne omembe in medijsko izpostavljenost, povezano z organizacijo.

4.2 vodja informacijske varnosti (CISO) / ekipa za informacijsko varnost

4.2.1 spremlja digitalne platforme za kazalnike uhajanja podatkov, lažnega predstavljanja ali poskusov ribarjenja,

4.2.2 se usklajuje z ekipami za odziv na incidente v primeru napadov ali kršitev, povezanih z družbenimi mediji.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Izvajanje in skladnost

9.1 Ta politika je obvezna za vse zajeto osebje in tretje osebe. Neupoštevanje lahko povzroči:

9.1.1 uradna opozorila,

9.1.2 začasen ali trajen preklic dostopa do platform ali sistemov,

9.1.3 disciplinske ukrepe, vključno s prenehanjem sodelovanja,

9.1.4 sodne postopke, če zunanje komuniciranje povzroči škodo za ugled, kršitev varnosti osebnih podatkov ali regulativno neskladnost.

9.2 Disciplinski ukrepi

9.2.1 Notranje kršitve (npr. razkritje zaupnih podatkov, obrekovanje organizacije) sprožijo vključitev kadrovske službe, formalno preiskavo in dokumentiranje v kadrovski evidenci zaposlenega.

9.2.2 Kadar je to ustrezno, pravna služba uveljavlja civilnopravna sredstva ali obvesti pristojne organe o kaznivih dejanjih (npr. lažno predstavljanje, razkritja v zvezi z notranjim trgovanjem).

9.3 Spremljanje skladnosti

9.3.1 Ekipi za informacijsko varnost in komuniciranje morata izvajati stalno spremljanje:

9.3.1.1 omemb blagovne znamke na glavnih platformah,

9.3.1.2 neuradne uporabe podob organizacije ali blagovnih znamk,

9.3.1.3 znanih tveganj (npr. nezadovoljni zaposleni, poskusi lažnega predstavljanja).

9.3.2 Spremljanje mora biti skladno z zakonodajo in predpisi o zasebnosti zaposlenih, vse zaznane primere pa mora preveriti človek.

9.4 Prijava nepravilnosti in neprimerne uporabe

9.4.1 Vsak zaposleni, ki sumi na kršitev te politike, se spodbuja, da to prijavi ekipi za informacijsko varnost, pravni službi ali anonimno prek portala za prijavo nepravilnosti.

9.4.2 Povračilni ukrepi proti prijaviteljem so strogo prepovedani in bodo predmet takojšnjih disciplinskih ukrepov.

10. Zahteve za pregled in posodobitev

10.1 Ta politika mora biti pregledana letno ali prej, če:

10.1.1 pride do pomembnih sprememb regulativnih zahtev (npr. nova zakonodaja EU o digitalnem komuniciranju),

10.1.2 se uvedejo nove družbene platforme ali komunikacijski kanali,

10.1.3 pride do pomembnega incidenta ali ponavljajočih se kršitev, ki kažejo na vrzeli v postopkih,

10.1.4 pride do organizacijske spremembe ali spremembe vodstva v funkcijah odnosov z javnostmi, pravne službe ali informacijske varnosti.

10.2 Pregled morajo skupaj izvesti:

10.2.1 vodja marketinga / odnosov z javnostmi,

10.2.2 vodja informacijske varnosti ali vodja tveganj informacijske varnosti,

10.2.3 nosilci funkcij pravne službe in skladnosti.

10.3 Posodobitve morajo biti dokumentirane v registru sprememb politike in sporočene prek notranjih kanalov ozaveščanja. Kadar pride do bistvenih sprememb, mora vse prizadeto osebje ponovno potrditi seznanitev s politiko.

11. Povezane politike in povezave

11.1 To politiko podpirajo in z njo so povezane naslednje komponente sistema upravljanja informacijske varnosti (ISMS) organizacije:

11.1.1 P1 – Politika informacijske varnosti: določa krovna načela za varovanje informacij, vključno z zagotavljanjem, da komuniciranje ne vodi do nepooblaščenega razkritja.

11.1.2 P3 – Politika sprejemljive uporabe (AUP): opredeljuje sprejemljivo ravnanje pri uporabi digitalnih platform in tehnologij, kar neposredno ureja osebno in profesionalno uporabo družbenih kanalov.

11.1.3 P6 – Politika upravljanja tveganj: določa okvir za obvladovanje tveganj pri ocenjevanju groženj, povezanih z javnim komuniciranjem in izpostavljenostjo ugleda.

11.1.4 P8 – Politika ozaveščanja in usposabljanja za informacijsko varnost: določa programe ozaveščanja, ki osebje seznanjajo z varnimi praksami komuniciranja in grožnjami socialnega inženiringa.

11.1.5 P13 – Politika klasifikacije in označevanja podatkov: usmerja osebje glede tega, kaj se šteje za omejene ali zaupne informacije, ki se ne smejo razkriti navzven.

11.1.6 P30 – Politika odzivanja na incidente: določa način obravnave incidentov, povezanih z javnim komuniciranjem, vključno z uhajanjem podatkov, lažnim predstavljanjem in regulativnimi kršitvami.

11.1.7 P33 – Politika spremljanja presoje in skladnosti: ureja procese presoje, s katerimi se preverjajo kontrole družbenih medijev, sistemi spremljanja in skladnost s politikami zunanjega komuniciranja.

12. Referenčni standardi in okviri

12.1 ISO/IEC 27001:

12.1.1 Klavzula 8.1 – operativno načrtovanje in obvladovanje: zahteva opredeljene procese in upravljanje na podlagi vlog za upravljanje javnega komuniciranja, ki zagotavljajo točnost, odobritvene poteke dela in eskalacijo incidentov, povezanih s podatki ali tveganjem za ugled.

12.2 ISO/IEC 27002:2022:

12.2.1 Kontrola 5.10 – uporaba informacij: ureja pooblaščeno in etično razširjanje notranjih ali zunanjih komunikacij.

12.2.2 Kontrola 5.11 – sprejemljiva uporaba informacij in drugih povezanih sredstev: krepi sprejemljive prakse za deljenje vsebin z uporabo sredstev organizacije ali osebnih računov.

12.2.3 Kontrola 5.35 – stik s pristojnimi organi: zahteva strukturirano in pooblaščeno zunanje komuniciranje z regulatornimi organi in javnimi institucijami.

12.2.4 Kontrola 5.36 – skladnost s politikami, pravili in standardi za informacijsko varnost: zahteva dosledno uporabo notranjih politik v vseh scenarijih komuniciranja.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – pravila vedenja: zahteva formalna pravila za uporabo sistemov in komunikacij, vključno s standardi javnega razkritja.

12.3.2 AC-8 – obvestilo o uporabi sistema: podpira obvezna obvestila in opozorila glede vsebine na zunanjih platformah.

12.3.3 AU-12 – ustvarjanje revizijskih zapisov: velja za ohranjanje dnevnikov in zgodovine komunikacij za namene pregleda incidentov in presoje.

12.4 Uredba EU GDPR (2016/679):

12.4.1 Člen 5 – načela obdelave osebnih podatkov: prepoveduje nepooblaščeno deljenje osebnih podatkov prek javnega komuniciranja.

12.4.2 Člen 25 – varstvo podatkov že pri načrtovanju in privzeto varstvo podatkov: zahteva varovala zasebnosti v komunikacijskih orodjih in potekih dela za vsebine.

12.4.3 Člen 32 – varnost obdelave: uporablja šifriranje, nadzor dostopa in procese odobritve vsebin.

12.4.4 Člen 33 – prijava kršitve varnosti osebnih podatkov: zahteva pravočasno razkritje uhajanj osebnih podatkov prek javnih kanalov.

12.5 Direktiva EU NIS2 (2022/2555):

12.5.1 Člen 21 – ukrepi za upravljanje tveganj kibernetske varnosti: vključuje komunikacijske protokole in obveznosti med incidenti ter javnim komuniciranjem o tveganjih.

12.6 Uredba EU DORA (2022/2554):

12.6.1 Člen 9 – upravljanje tveganj IKT: velja za komunikacijska tveganja, ki izvirajo od zunaj, kot so lažno predstavljanje, dezinformacije in motenje ugleda.

12.6.2 Člen 16 – komunikacijska strategija: zahteva, da kritični finančni subjekti ali ponudniki storitev v kriznih scenarijih upravljajo komunikacijska tveganja in odzive.

12.7 COBIT 2019:

12.7.1 APO09 – upravljani sporazumi o storitvah in komuniciranje: zahteva strukturirano upravljanje notranjih in zunanjih komunikacij.

12.7.2 DSS05 – upravljanje varnostnih storitev: zagotavlja, da komunikacijske dejavnosti ne uvajajo dodatnega tveganja in ne slabijo procesov obravnave incidentov.