					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	Klavzule 5.1, 5.2, 6.1, 8	Vodenje, obvladovanje tveganj in operativni nadzor nad zunanjim komuniciranjem
ISO/IEC 27002:2022	Kontroli 5.10, 5.11	Sprejemljiva uporaba in informacijska varnost pri komuniciranju
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Pravila ravnanja, revizija, poročanje o incidentih ter upravljanje javno dostopnih vsebin in dostopa
Uredba EU GDPR	Členi 5, 32, 33	Načela varstva osebnih podatkov, varnost in obveščanje o kršitvah, ki vplivajo na javno komuniciranje
Direktiva EU NIS2	Člen 21(2)(e), 21(2)(f)	Politike uporabe sistemov ter obvladovanje tveganj v dobavni verigi in tveganj javnega komuniciranja
Uredba EU DORA	Člen 14(4)	Obveznosti komuniciranja po incidentih

1. Namen

1.1. Ta politika določa obvezna pravila za vse oblike javnega komuniciranja, vključno z uporabo družbenih medijev, sodelovanjem z mediji in zunanjimi digitalnimi vsebinami, kadar se nanašajo na podjetje, njegove zaposlene, stranke, sisteme ali notranje prakse.

1.2. Politika podpira varovanje ugleda podjetja, zagotavljanje skladnosti s pravnimi in regulativnimi zahtevami ter zmanjševanje tveganja uhajanja podatkov, dezinformacij ali varnostnih incidentov.

1.3. Zaposlenim in partnerjem omogoča pozitivno in odgovorno sodelovanje v spletnih razpravah ter hkrati preprečuje nenamerna razkritja ali napačno predstavljanje.

1.4. Politika krepi pripravljenost SME na certifikacijo po ISO/IEC 27001 z obravnavo nadzora nad informacijami, ki so dane na voljo javnosti ali zunanjim zainteresiranim stranem.

2. Področje uporabe

2.1. Ta politika velja za vse osebe, povezane z organizacijo, vključno z:

2.1.1. zaposlenimi in pogodbenimi izvajalci,

2.1.2. samostojnimi izvajalci, svetovalci in dobavitelji tretjih oseb,

2.1.3. praktikanti ali zaposlenimi s krajšim delovnim časom, ki sodelujejo pri izvajanju storitev za stranke ali imajo dostop do sistemov.

2.2. Politika velja za vse oblike zunanjega komuniciranja, ki se nanašajo na organizacijo, vključno z:

2.2.1. objavami na družbenih medijih (LinkedIn, Twitter/X, TikTok, Instagram, Facebook itd.),

2.2.2. objavami na blogih, spletnimi forumi, ocenami strank in razpravami,

2.2.3. javnimi nastopi (npr. konference, spletni seminarji, podkasti),

2.2.4. e-poštnimi sporočili ali sporočili novinarjem, predstavnikom državnih organov ali vplivnežem,

2.2.5. javno deljenimi posnetki zaslona, fotografijami ali videoposnetki iz delovnih okolij.

2.3. Politika velja tudi, kadar se takšno komuniciranje izvaja:

2.3.1. z osebnih naprav ali računov,

2.3.2. zunaj običajnega delovnega časa,

2.3.3. brez zlonamernega namena — tudi nenamerne ali mimogrede podane izjave spadajo v področje uporabe te politike, če se nanašajo na podjetje.

3. Cilji

3.1. Varovanje ugleda: preprečiti škodo ugledu podjetja zaradi nepooblaščenega ali neustreznega javnega komuniciranja.

3.2. Varnost podatkov: preprečiti nenamerno razkritje občutljivih podatkov, informacij o notranjih sistemih ali podatkov o strankah prek družbenih medijev ali javnih kanalov.

3.3. Pravna in regulativna skladnost: zagotoviti, da so vse javne vsebine, ki se nanašajo na podjetje, skladne z veljavno zakonodajo s področja varstva podatkov in poslovnega komuniciranja.

3.4. Profesionalno ravnanje: spodbujati odgovorno sodelovanje v spletnih razpravah in nastopih v medijih, tudi pri uporabi osebnih računov.

3.5. Pripravljenost na incidente: zagotoviti jasne in izvedljive korake v primeru nenamernih razkritij ali kršitev politike.

4. Vloge in odgovornosti

4.1. Generalni direktor (GM)

4.1.1. je lastnik te politike in jo odobri,

4.1.2. pregleda in odobri vse javne izjave, sodelovanje z mediji in medijske intervjuje,

4.1.3. zagotovi, da je ta politika jasno sporočena vsem zaposlenim in tretjim osebam,

4.1.4. v usklajevanju s postopki odzivanja na incidente preiskuje in obravnava vse kršitve te politike.

4.2. Določeni zaposleni ali vodja komuniciranja (če je imenovan)

4.2.1. podpira GM pri pregledu vsebin pred zunanjo objavo (npr. objav na blogih, tem za nastope),

4.2.2. vodi evidence odobrenih medijskih aktivnosti ali objav na družbenih medijih z višjo stopnjo tveganja,

4.2.3. v okviru razpoložljivih zmogljivosti spremlja znane omembe podjetja na spletu zaradi tveganj za ugled ali varnost.

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

9. Zahteve za pregled in posodabljanje

9.1. Letni pregled

9.1.1. To politiko mora najmanj enkrat letno pregledati generalni direktor (GM).

9.1.2. Pregled mora zagotoviti usklajenost s posodobljenimi pravnimi obveznostmi, trendi komuniciranja v panogi in notranjimi poslovnimi spremembami.

9.2. Pregledi na podlagi sprožilcev

9.2.1. Ta politika mora biti nemudoma posodobljena po:

9.2.1.1. pomembnem incidentu na družbenih medijih ali vprašanju ugleda,

9.2.1.2. spremembi dobaviteljev tretjih oseb, ki upravljajo komuniciranje,

9.2.1.3. novi zakonodaji ali regulativnih obveznostih, povezanih s spletnim komuniciranjem, mediji ali blagovno znamko.

9.3. Dokumentiranje sprememb

9.3.1. Vse posodobitve morajo biti evidentirane, vključno z datumom revizije, povzetkom sprememb in odobritvijo GM.

9.3.2. Za potrebe presoje in certifikacije je treba voditi evidenco različic.

9.4. Razširjanje posodobitev

9.4.1. Vsi zaposleni in pogodbeni izvajalci morajo biti obveščeni o vsaki spremembi politike.

9.4.2. Posodobljene različice morajo biti posredovane po e-pošti ali prek internih portalov.

9.4.3. Vsak dobavitelj, ki izvaja javno komuniciranje, mora pred nadaljevanjem dela potrditi posodobljene pogoje.

10. Povezane politike in povezave

10.1. Ta politika se izvaja v povezavi z naslednjimi politikami SME:

10.1.1. P3S – Politika sprejemljive uporabe (AUP): določa sprejemljivo ravnanje pri uporabi komunikacijskih platform, vključno z dostopom do družbenih medijev med delovnim časom.

10.1.2. P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da so zaposleni usposobljeni za prepoznavanje tveganj prekomernega deljenja vsebin, napadov z lažnim predstavljanjem ali spletnih groženj za ugled.

10.1.3. P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da se osebni podatki in podatki o strankah ne delijo v zunanjem komuniciranju ter da je ravnanje usklajeno z GDPR in drugimi pravnimi zahtevami.

10.1.4. P30S – Politika odzivanja na incidente: ureja odziv na nenamerno javno razkritje, spletne grožnje ali napade na ugled, ki izhajajo iz neustrezne uporabe družbenih medijev.

10.1.5. P37S – Politika pravne in regulativne skladnosti: določa širše pravne in pogodbene obveznosti organizacije pri javni objavi vsebin.

10.2. Te politike se morajo uporabljati skupaj, da se zagotovi varna, spoštljiva in pravno skladna zunanja prisotnost.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 5.1 – Vodenje in zavezanost: zahteva vodstveni nadzor nad tveganji za ugled in informacijskimi tveganji.

11.1.2. Klavzula 6.1 – Obvladovanje tveganj: vključuje izpostavljenosti tveganjem, povezanim s komuniciranjem.

11.1.3. Klavzula 8.1 – Operativni nadzor: zajema pravila za zunanje komuniciranje informacij.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.10 – Sprejemljiva uporaba sredstev podjetja.

11.2.2. Kontrola 5.11 – Informacijska varnost pri komuniciranju.

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Pravila ravnanja: ureja ustrezno ravnanje pri uporabi informacijskih virov.

11.3.2. AU-7 – Zmanjšanje obsega revizijskih podatkov in priprava poročil: podpira spremljanje javne uporabe sistemov.

11.3.3. IR-6 – Poročanje o incidentih: zahteva odziv na kršitve, povezane z ugledom in komuniciranjem.

11.3.4. AC-22 – Javno dostopna vsebina: zagotavlja nadzor nad zunanjimi objavami in dostopom.

11.4. Uredba EU GDPR (2016/679)

11.4.1. Člen 5 – Načela v zvezi z obdelavo osebnih podatkov (točnost, celovitost in zaupnost, odgovornost).

11.4.2. Člen 32 – Varnost obdelave: zahteva zaščitne ukrepe pri javnem deljenju.

11.4.3. Člen 33 – Obveščanje o kršitvah: se sproži, če so osebni podatki izpostavljeni prek zunanjega komuniciranja.

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Člen 21(2)(e) – Politike uporabe informacijskih sistemov, vključno s komunikacijskimi platformami.

11.5.2. Člen 21(2)(f) – Politike za obravnavo tveganj kibernetske varnosti v dobavni verigi in na javnih platformah.

11.6. Uredba EU DORA (2022/2554)

11.6.1. Člen 14(4) – Obveznosti komuniciranja do strank, tretjih oseb in organov po operativnih incidentih.

11.7. COBIT 2019

11.7.1. APO09 – Upravljanje sporazumov o ravni storitev: zajema nadzor nad dobavitelji in tretjimi osebami, povezanimi s komuniciranjem.

11.7.2. DSS05 – Upravljanje varnostnih storitev: vključuje zaščito javno izpostavljenih digitalnih sredstev.

11.7.3. EDM03 – Zagotavljanje optimizacije tveganj: poudarja obvladovanje tveganj za ugled in skladnost, povezanih s komuniciranjem.