					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P36S					Naziv dokumenta: **Politika društvenih mreža i vanjske komunikacije**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Pravna napomena (autorska prava i ograničenja uporabe)

(C) 2025 Clarysec LLC. All rights reserved.

Ovaj dokument intelektualno je vlasništvo društva Clarysec LLC. Nijedan dio ovog dokumenta ne smije se kopirati, ponovno upotrebljavati, distribuirati niti mijenjati u komercijalne svrhe ili svrhe implementacije bez izričitog prethodnog pisanog odobrenja.

Neovlaštena uporaba strogo je zabranjena i može rezultirati pravnim postupkom.

Za licenciranje kontaktirajte: info@clarysec.com

Usklađeno sa standardima i propisima

Standard/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.1, 5.2, 6.1, 8	Vodstvo, upravljanje rizicima i operativno upravljanje vanjskom komunikacijom
ISO/IEC 27002:2022	Kontrole 5.10, 5.11	Prihvatljiva uporaba i informacijska sigurnost u komunikaciji
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Pravila ponašanja, revizija, prijava incidenata te upravljanje javno dostupnim sadržajem i pristupom
GDPR EU	Članci 5, 32, 33	Načela zaštite podataka, sigurnost i prijava povrede osobnih podataka koja utječe na javnu komunikaciju
Direktiva EU NIS2	Članak 21(2)(e), 21(2)(f)	Politike korištenja sustava te upravljanje rizicima opskrbnog lanca i javne komunikacije
Uredba EU DORA	Članak 14(4)	Obveze komunikacije nakon incidenata

1. Svrha

1.1. Ova politika utvrđuje obvezna pravila za svu javnu komunikaciju, uključujući korištenje društvenih mreža, komunikaciju s medijima i vanjski digitalni sadržaj, kada se odnosi na društvo, njegovo osoblje, klijente, sustave ili interne prakse.

1.2. Ova politika pomaže zaštititi ugled društva, održati usklađenost sa zakonskim i regulatornim zahtjevima te smanjiti rizik od curenja informacija, dezinformacija ili sigurnosnih incidenata.

1.3. Politika omogućuje zaposlenicima i partnerima pozitivno i odgovorno sudjelovanje u internetskim raspravama, uz izbjegavanje nenamjernog otkrivanja informacija ili pogrešnog predstavljanja.

1.4. Ova politika jača spremnost SME-a za certifikaciju prema normi ISO/IEC 27001 uređivanjem kontrole informacija koje se stavljaju na raspolaganje javnosti ili vanjskim dionicima.

2. Područje primjene

2.1. Ova politika primjenjuje se na sve osobe povezane s organizacijom, uključujući:

2.1.1. zaposlenike i ugovorne izvršitelje

2.1.2. vanjske suradnike, savjetnike i dobavljače trećih strana

2.1.3. pripravnike i zaposlenike s nepunim radnim vremenom uključene u isporuku usluga klijentima ili s pristupom sustavima

2.2. Ova politika primjenjuje se na sve oblike vanjske komunikacije koji se odnose na organizaciju, uključujući:

2.2.1. objave na društvenim mrežama (LinkedIn, Twitter/X, TikTok, Instagram, Facebook itd.)

2.2.2. objave na blogovima, internetskim forumima, korisničke recenzije i rasprave

2.2.3. javne nastupe (npr. konferencije, webinare, podcaste)

2.2.4. e-poštu ili poruke novinarima, predstavnicima državnih tijela ili influencerima

2.2.5. javno podijeljene snimke zaslona, fotografije ili videozapise iz radnog okruženja

2.3. Ova politika primjenjuje se i kada se takva komunikacija odvija:

2.3.1. s osobnih uređaja ili računa

2.3.2. izvan uobičajenog radnog vremena

2.3.3. bez zlonamjerne namjere — čak i slučajne ili usputne izjave obuhvaćene su ovom politikom ako se odnose na društvo

3. Ciljevi

3.1. Zaštita ugleda: spriječiti narušavanje ugleda društva zbog neovlaštene ili neprimjerene javne komunikacije

3.2. Sigurnost podataka: izbjeći nenamjerno izlaganje osjetljivih podataka, internih sustava ili podataka o klijentima putem društvenih mreža ili javnih kanala

3.3. Usklađenost sa zakonskim i regulatornim zahtjevima: osigurati da je sav javno dostupan sadržaj koji se odnosi na društvo usklađen s primjenjivim propisima o zaštiti podataka i poslovnoj komunikaciji

3.4. Profesionalno postupanje: poticati odgovorno sudjelovanje u internetskim raspravama i komunikaciji s medijima, uključujući i putem osobnih računa

3.5. Spremnost za incidente: osigurati jasne i provedive korake u slučaju slučajnog otkrivanja informacija ili kršenja politike

4. Uloge i odgovornosti

4.1. Glavni direktor (GM)

4.1.1. vlasnik je ove politike i odobrava je

4.1.2. pregledava i odobrava sve javne izjave, komunikaciju s medijima i medijske intervjue

4.1.3. osigurava da se ova politika jasno priopći svim zaposlenicima i trećim stranama

4.1.4. istražuje svako kršenje ove politike i poduzima odgovarajuće mjere u koordinaciji s postupcima odgovora na incidente

4.2. Imenovani zaposlenik ili voditelj komunikacija (ako je određen)

4.2.1. pruža podršku GM-u pregledom sadržaja prije vanjske objave (npr. blog objave, teme za javni nastup)

4.2.2. vodi evidenciju o odobrenim medijskim aktivnostima ili objavama na društvenim mrežama visokog rizika

4.2.3. prati poznata spominjanja društva na internetu radi utvrđivanja rizika za ugled ili sigurnost, u mjeri u kojoj to kapaciteti dopuštaju

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1. Godišnji pregled

9.1.1. Ovu politiku mora pregledati najmanje jednom godišnje glavni direktor (GM)

9.1.2. Pregled mora osigurati usklađenost s ažuriranim zakonskim obvezama, komunikacijskim trendovima u industriji i internim poslovnim promjenama

9.2. Pregledi potaknuti događajem

9.2.1. Ova politika mora se ažurirati odmah nakon:

9.2.1.1. značajnog incidenta na društvenim mrežama ili problema povezanog s ugledom

9.2.1.2. promjene dobavljača treće strane koji upravlja komunikacijom

9.2.1.3. novih zakona ili regulatornih obveza povezanih s internetskom komunikacijom, medijima ili brendom

9.3. Dokumentiranje promjena

9.3.1. Sva ažuriranja moraju se evidentirati, uključujući datum izmjene, sažetak promjena i odobrenje GM-a

9.3.2. Mora se voditi povijest verzija za potrebe revizije i certifikacije

9.4. Distribucija ažuriranja

9.4.1. Svo osoblje i ugovorni izvršitelji moraju biti obaviješteni o svakoj promjeni politike

9.4.2. Ažurirane verzije moraju se distribuirati putem e-pošte ili internih portala

9.4.3. Svaki dobavljač koji pruža usluge javne komunikacije mora potvrditi prihvaćanje ažuriranih uvjeta prije nastavka rada

10. Povezane politike i poveznice

10.1. Ova politika primjenjuje se u koordinaciji sa sljedećim SME politikama:

10.1.1. P3S – Politika prihvatljive uporabe: definira prihvatljivo ponašanje pri korištenju komunikacijskih platformi, uključujući pristup društvenim mrežama tijekom radnog vremena

10.1.2. P8S – Politika podizanja svijesti o informacijskoj sigurnosti i osposobljavanja: osigurava da je osoblje osposobljeno za prepoznavanje rizika prekomjernog dijeljenja informacija, phishinga ili prijetnji ugledu na internetu

10.1.3. P17S – Politika zaštite podataka i privatnosti: osigurava da se osobni podaci i podaci o klijentima ne dijele u vanjskoj komunikaciji, u skladu s GDPR-om i drugim zakonskim zahtjevima

10.1.4. P30S – Politika odgovora na incidente: uređuje odgovor na slučajno javno otkrivanje podataka, internetske prijetnje ili napade na ugled koji proizlaze iz neprimjerene uporabe društvenih mreža

10.1.5. P37S – Politika pravne i regulatorne usklađenosti: utvrđuje šire pravne i ugovorne obveze organizacije pri javnoj objavi sadržaja

10.2. Ove politike moraju se primjenjivati zajedno kako bi se održala sigurna, profesionalna i pravno usklađena vanjska prisutnost.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 5.1 – Vodstvo i opredijeljenost: zahtijeva nadzor vodstva nad reputacijskim i informacijskim rizicima

11.1.2. Točka 6.1 – Upravljanje rizicima: uključuje izloženosti rizicima povezanima s komunikacijom

11.1.3. Točka 8.1 – Operativno upravljanje: obuhvaća pravila o tome kako se informacije komuniciraju prema vanjskim stranama

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.10 – Prihvatljiva uporaba informacija i imovine

11.2.2. Kontrola 5.11 – Informacijska sigurnost u komunikaciji

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Pravila ponašanja: uređuje primjereno postupanje pri korištenju informacijskih resursa

11.3.2. AU-7 – Smanjenje opsega revizijskih podataka i generiranje izvješća: podupire praćenje javne uporabe sustava

11.3.3. IR-6 – Prijava incidenata: nalaže odgovor na povrede povezane s ugledom i komunikacijom

11.3.4. AC-22 – Javno dostupan sadržaj: osigurava kontrolu nad vanjskim objavama i pristupom

11.4. GDPR EU (2016/679)

11.4.1. Članak 5 – Načela obrade osobnih podataka (točnost, cjelovitost, odgovornost)

11.4.2. Članak 32 – Sigurnost obrade: zahtijeva zaštitne mjere pri javnom dijeljenju podataka

11.4.3. Članak 33 – Prijava povrede osobnih podataka: primjenjuje se ako su osobni podaci izloženi vanjskom komunikacijom

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Članak 21(2)(e) – Politike korištenja informacijskih sustava, uključujući komunikacijske platforme

11.5.2. Članak 21(2)(f) – Politike za upravljanje kibernetičkim rizicima u opskrbnom lancu i na javnim platformama

11.6. Uredba EU DORA (2022/2554)

11.6.1. Članak 14(4) – Obveze komunikacije prema klijentima, trećim stranama i nadležnim tijelima nakon operativnih incidenata

11.7. COBIT 2019

11.7.1. APO09 – Upravljanje ugovorima o uslugama: obuhvaća nadzor nad dobavljačima i trećim stranama povezanima s komunikacijom

11.7.2. DSS05 – Upravljanje sigurnosnim uslugama: uključuje zaštitu javno dostupne digitalne imovine

11.7.3. EDM03 – Osiguravanje optimizacije rizika: naglašava upravljanje reputacijskim rizicima i rizicima usklađenosti povezanima s komunikacijom