					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**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Definirani procesi i upravljanje temeljeno na ulogama za upravljanje javnom komunikacijom, uz osiguranje točnosti, tijekova odobravanja i eskalacije incidenata.
ISO/IEC 27002:2022	Kontrole 5.10, 5.11, 5.35, 5.36	Uređuje uporabu, prihvatljivu uporabu te vanjsku komunikaciju s tijelima vlasti i izvješćivanje o usklađenosti.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Pravila uporabe sustava i komunikacija, obavještavanje korisnika i čuvanje revizijskih zapisa.
GDPR EU	Članci 5, 25, 32, 33	Načela obrade podataka, zaštita podataka već u fazi projektiranja, sigurnost obrade i obveze prijave povrede.
Direktiva EU NIS2	Članak 21	Mjere upravljanja rizicima kibernetičke sigurnosti, obveze u slučaju incidenata i javne komunikacije povezane s rizikom.
Uredba EU DORA	Članci 9, 16	Upravljanje IKT rizicima i komunikacijska strategija za kritične pružatelje usluga.
COBIT 2019	APO09, DSS05	Upravljanje ugovorima o razini usluge i komunikacijom te sigurne komunikacijske prakse i upravljanje incidentima.

1. Svrha

1.1 Ova politika uspostavlja obvezna pravila i odgovornosti kojima se uređuje uporaba društvenih mreža i svi oblici vanjske komunikacije osoblja povezanog s organizacijom.

1.2 Njome se osigurava da su javne poruke — planirane ili spontane — točne, primjerene, sigurne, usklađene sa zakonskim zahtjevima i usklađene s identitetom brenda.

1.3 Svrha ove politike jest smanjiti rizike povezane s reputacijskom štetom, regulatornim povredama, gubitkom intelektualnog vlasništva i neovlaštenim objavama putem javno dostupnih kanala.

1.4 Ova politika dodatno promiče odgovornost i strukturirano upravljanje svim oblicima digitalne komunikacije koji uključuju organizaciju ili na nju utječu.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve zaposlenike, ugovorne izvođače, vježbenike i predstavnike trećih strana koji:

2.1.1 Komuniciraju u ime organizacije, službeno ili neslužbeno

2.1.2 U javnom okruženju navode ili impliciraju povezanost s organizacijom

2.1.3 Koriste osobne ili korporativne račune za sudjelovanje u javnim raspravama koje uključuju organizaciju

2.2 Obuhvaćeni komunikacijski kanali uključuju, ali nisu ograničeni na:

2.2.1 Platforme društvenih mreža (npr. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blogove, wikije, forume i javne raspravne ploče

2.2.3 E-poštu ili izravne poruke vanjskim stranama (npr. klijentima, regulatorima, medijima)

2.2.4 Intervjue za medije, panel-rasprave ili snimljena medijska pojavljivanja

2.2.5 Sudjelovanje u internetskim zajednicama u kojima se spominje organizacija

2.3 Ova politika uređuje sadržaj objavljen u stvarnom vremenu i unaprijed zakazan sadržaj te se primjenjuje na sve uređaje i račune (osobne ili korporativne) koji se koriste za distribuciju komunikacije.

3. Ciljevi

3.1 Spriječiti slučajno ili namjerno otkrivanje povjerljivih, osjetljivih ili reguliranih informacija putem kanala vanjske komunikacije.

3.2 Osigurati da su službene javne izjave i sadržaj na društvenim mrežama točni, odobreni i usklađeni s korporativnim brendom, etičkim načelima i strateškim porukama.

3.3 Spriječiti reputacijsku štetu i osigurati dosljednost poruka između internih odjela i vanjskih platformi.

3.4 Ispuniti primjenjive zakonske obveze povezane s javnim izjavama, uključujući, ali ne ograničavajući se na GDPR, NIS2, DORA i sektorska pravila komunikacije.

3.5 Definirati jasne odgovornosti, dopuštene slučajeve uporabe i provedbene protokole za svo osoblje uključeno u aktivnosti usmjerene prema javnosti.

4. Uloge i odgovornosti

4.1 Glavni direktor marketinga ili komunikacija / voditelj odnosa s javnošću

4.1.1 Odobrava sve službene poruke društva za vanjsku objavu

4.1.2 Održava raspored objava na društvenim mrežama i smjernice radi dosljednosti brenda

4.1.3 Prati internetska spominjanja i medijsku izloženost povezanu s organizacijom

4.2 Glavni službenik za informacijsku sigurnost (CISO) / tim za informacijsku sigurnost

4.2.1 Prati digitalne platforme radi pokazatelja curenja podataka, lažnog predstavljanja ili pokušaja phishinga

4.2.2 Koordinira s timovima za odgovor na incidente u slučaju napada ili povreda povezanih s društvenim mrežama

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

9. Provedba i usklađenost

9.1 Ova politika obvezna je za svo obuhvaćeno osoblje i treće strane. Nepoštivanje može rezultirati:

9.1.1 Formalnim upozorenjem

9.1.2 Privremenim ili trajnim ukidanjem pristupa platformama ili sustavima

9.1.3 Stegovnim mjerama, uključujući prestanak radnog odnosa

9.1.4 Pravnim postupcima ako vanjska komunikacija rezultira reputacijskom štetom, povredom podataka ili regulatornom neusklađenošću

9.2 Stegovne mjere

9.2.1 Interna kršenja (npr. curenje povjerljivih podataka, klevetanje organizacije) pokrenut će uključivanje HR-a, formalnu istragu i dokumentiranje u dosjeu zaposlenika.

9.2.2 Gdje je primjenjivo, pravni poslovi poduzet će građanskopravne mjere ili obavijestiti nadležna tijela o kaznenim aktivnostima (npr. lažno predstavljanje, curenje informacija povezanih s insajderskim trgovanjem).

9.3 Praćenje usklađenosti

9.3.1 Timovi za sigurnost i komunikacije moraju kontinuirano pratiti:

9.3.1.1 Spominjanja brenda na glavnim platformama

9.3.1.2 Neslužbenu uporabu slika društva ili žigova

9.3.1.3 Poznate rizike (npr. nezadovoljni zaposlenici, pokušaji lažnog predstavljanja)

9.3.2 Praćenje mora biti usklađeno sa zakonima i propisima o privatnosti zaposlenika, a sve označene slučajeve mora provjeriti osoba zadužena za pregled.

9.4 Mehanizam za prijavu nepravilnosti i prijavu zlouporabe

9.4.1 Svaki zaposlenik koji sumnja na kršenje ove politike potiče se da to prijavi timu za informacijsku sigurnost, pravnim poslovima ili anonimno putem portala za prijavu nepravilnosti.

9.4.2 Odmazda protiv prijavitelja nepravilnosti strogo je zabranjena i podliježe trenutačnim stegovnim mjerama.

10. Zahtjevi za pregled i ažuriranje

10.1 Ova politika mora se pregledavati najmanje jednom godišnje ili ranije ako:

10.1.1 Dođe do značajnih promjena regulatornih zahtjeva (npr. novih propisa EU o digitalnim komunikacijama)

10.1.2 Budu uvedene nove društvene platforme ili komunikacijski kanali

10.1.3 Dođe do značajnog incidenta ili ponovljenih kršenja koja upućuju na manjkavosti u procesu

10.1.4 Dođe do strukturne promjene ili promjene vodstva u funkcijama odnosa s javnošću, pravnih poslova ili sigurnosti

10.2 Pregled moraju zajednički provesti:

10.2.1 Voditelj marketinga / odnosa s javnošću

10.2.2 CISO ili voditelj sigurnosnih rizika

10.2.3 Službenici za pravne poslove i usklađenost

10.3 Ažuriranja moraju biti dokumentirana u registru promjena politike i priopćena putem internih kanala za podizanje svijesti. Ako nastupe značajne promjene, svo zahvaćeno osoblje mora ponovno potvrditi upoznatost s politikom.

11. Povezane politike i poveznice

11.1 Ovu politiku podupiru i s njom su povezane sljedeće sastavnice sustava upravljanja informacijskom sigurnošću (ISMS) organizacije:

11.1.1 P1 – Politika informacijske sigurnosti: Uspostavlja krovna načela za zaštitu informacija, uključujući osiguravanje da komunikacija ne dovede do neovlaštenog otkrivanja.

11.1.2 P3 – Politika prihvatljive uporabe: Definira prihvatljiva ponašanja za digitalne platforme i tehnologije, koja izravno uređuju osobnu i profesionalnu uporabu društvenih kanala.

11.1.3 P6 – Politika upravljanja rizicima: Pruža okvir za upravljanje rizicima za procjenu prijetnji povezanih s javnom komunikacijom i reputacijskom izloženošću.

11.1.4 P8 – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: Propisuje programe podizanja svijesti kojima se osoblje educira o sigurnim komunikacijskim praksama i prijetnjama socijalnog inženjeringa.

11.1.5 P13 – Politika klasifikacije podataka i označavanja: Daje smjernice osoblju o tome što se smatra ograničenim ili povjerljivim informacijama koje se ne smiju objavljivati izvan organizacije.

11.1.6 P30 – Politika odgovora na incidente: Definira postupanje s incidentima povezanima s javnom komunikacijom, uključujući curenje podataka, lažno predstavljanje i regulatornu povredu.

11.1.7 P33 – Politika praćenja revizije i usklađenosti: Uređuje revizijske procese kojima se potvrđuju kontrole društvenih mreža, sustavi praćenja i usklađenost s politikama vanjske komunikacije.

12. Referentni standardi i okviri

12.1 ISO/IEC 27001:

12.1.1 Točka 8.1 – Operativno planiranje i kontrola: Zahtijeva definirane procese i upravljanje temeljeno na ulogama za upravljanje javnom komunikacijom, uz osiguranje točnosti, tijekova odobravanja i eskalacije incidenata koji uključuju podatke ili reputacijski rizik.

12.2 ISO/IEC 27002:2022:

12.2.1 Kontrola 5.10 – Uporaba informacija: Uređuje ovlašteno i etično dijeljenje internih ili vanjskih komunikacija.

12.2.2 Kontrola 5.11 – Prihvatljiva uporaba informacija i imovine: Jača prihvatljive prakse za dijeljenje sadržaja uporabom korporativne imovine ili osobnih računa.

12.2.3 Kontrola 5.35 – Kontakt s tijelima vlasti: Zahtijeva strukturiranu i ovlaštenu vanjsku komunikaciju s regulatornim tijelima i javnim ustanovama.

12.2.4 Kontrola 5.36 – Usklađenost s politikama i standardima: Osigurava dosljednu primjenu internih politika u svim komunikacijskim scenarijima.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Pravila ponašanja: Zahtijeva formalna pravila za uporabu sustava i komunikacija, uključujući standarde javne objave.

12.3.2 AC-8 – Obavijest o uporabi sustava: Podržava obvezne izjave o odricanju od odgovornosti i upozorenja o sadržaju na izvana dostupnim platformama.

12.3.3 AU-12 – Čuvanje revizijskih zapisa: Primjenjuje se na očuvanje dnevničkih zapisa i povijesti komunikacije za potrebe pregleda incidenata i revizije.

12.4 GDPR EU (2016/679):

12.4.1 Članak 5 – Načela obrade podataka: Zabranjuje neovlašteno dijeljenje osobnih podataka putem javne komunikacije.

12.4.2 Članak 25 – Zaštita podataka već u fazi projektiranja i zaštita podataka prema zadanim postavkama: Zahtijeva zaštitne mjere privatnosti u komunikacijskim alatima i tijekovima sadržaja.

12.4.3 Članak 32 – Sigurnost obrade: Primjenjuje šifriranje, kontrolu pristupa i procese odobravanja sadržaja.

12.4.4 Članak 33 – Prijava povrede: Propisuje pravodobnu prijavu curenja osobnih podataka putem javnih kanala.

12.5 Direktiva EU NIS2 (2022/2555):

12.5.1 Članak 21 – Mjere upravljanja rizicima kibernetičke sigurnosti: Uključuje komunikacijske protokole i obveze tijekom incidenata i javne komunikacije povezane s rizikom.

12.6 Uredba EU DORA (2022/2554):

12.6.1 Članak 9 – Upravljanje IKT rizicima: Primjenjuje se na izvana potaknute komunikacijske rizike kao što su lažno predstavljanje, dezinformacije i narušavanje reputacije.

12.6.2 Članak 16 – Komunikacijska strategija: Zahtijeva da kritični financijski ili uslužni pružatelji upravljaju komunikacijskim rizicima i odgovorima u kriznim scenarijima.

12.7 COBIT 2019:

12.7.1 APO09 – Upravljanje ugovorima o uslugama i komunikacijom: Zahtijeva strukturirano upravljanje internom i vanjskom komunikacijom.

12.7.2 DSS05 – Upravljanje sigurnosnim uslugama: Osigurava da komunikacijske aktivnosti ne uvode dodatni rizik niti narušavaju postupanje s incidentima.