					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P36S					Dokumenta nosaukums: **Sociālo mediju un ārējās komunikācijas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Nosaka procesus un lomās balstītu pārvaldību publiskās komunikācijas pārvaldībai, nodrošinot precizitāti, apstiprināšanas darbplūsmas un incidentu eskalāciju.
ISO/IEC 27002:2022	5.10., 5.11., 5.35., 5.36. kontrole	Regulē informācijas izmantošanu, pieļaujamo lietošanu, kā arī saziņu ar ārējām kontaktpersonām vai iestādēm un atbilstības ziņošanu.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Sistēmu un komunikācijas izmantošanas noteikumi, lietotāju paziņojumi, audita ierakstu saglabāšana.
ES VDAR	5., 25., 32., 33. pants	Datu apstrādes principi, datu aizsardzība pēc projektēšanas un pēc noklusējuma, apstrādes drošība, pienākums paziņot par pārkāpumu.
ES NIS2	21. pants	Kiberdrošības risku pārvaldības pasākumi, pienākumi incidentu gadījumā un ar risku saistīta publiskā komunikācija.
ES DORA	9., 16. pants	IKT risku pārvaldība un komunikācijas stratēģija kritiski svarīgiem pakalpojumu sniedzējiem.
COBIT 2019	APO09, DSS05	Pakalpojumu līmeņa vienošanos un komunikācijas pārvaldība, kā arī drošas komunikācijas prakse un incidentu pārvaldība.

1. Mērķis

1.1 Šī politika nosaka obligātus noteikumus un pienākumus, kas reglamentē sociālo mediju un visu ārējās komunikācijas veidu izmantošanu personām, kuras ir saistītas ar organizāciju.

1.2 Tā nodrošina, ka publiskā komunikācija neatkarīgi no tā, vai tā ir plānota vai spontāna, ir precīza, cieņpilna, droša, atbilstoša tiesiskajām prasībām un saskaņota ar zīmola vadlīnijām.

1.3 Politikas mērķis ir mazināt riskus, kas saistīti ar reputācijas kaitējumu, regulatīvo prasību pārkāpumiem, intelektuālā īpašuma neatļautu izpaušanu un nesankcionētu informācijas atklāšanu publiski pieejamos kanālos.

1.4 Tāpat politika veicina pārskatatbildību un strukturētu pārvaldību visos digitālās komunikācijas veidos, kas ir saistīti ar organizāciju vai to ietekmē.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem darbiniekiem, līgumdarbiniekiem, praktikantiem un trešo personu pārstāvjiem, kuri:

2.1.1 komunicē organizācijas vārdā oficiāli vai neoficiāli;

2.1.2 publiskā vidē atsaucas uz saistību ar organizāciju vai rada šādu iespaidu;

2.1.3 izmanto personīgos vai uzņēmuma kontus, lai iesaistītos publiskās diskusijās, kas saistītas ar organizāciju.

2.2 Politikas aptvertie komunikācijas kanāli ietver, bet neaprobežojas ar:

2.2.1 sociālo mediju platformām (piemēram, LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook);

2.2.2 emuāriem, vikivietnēm, forumiem un publiskām diskusiju platformām;

2.2.3 e-pastu vai tiešo ziņapmaiņu ar ārējām pusēm (piemēram, klientiem, regulatoriem, plašsaziņas līdzekļiem);

2.2.4 preses intervijām, uzstāšanos paneļdiskusijās vai ierakstītām uzstāšanās reizēm medijos;

2.2.5 dalību tiešsaistes kopienās, kurās tiek pieminēta organizācija.

2.3 Šī politika reglamentē gan reāllaika, gan iepriekš ieplānotu saturu un attiecas uz visām ierīcēm un kontiem (personīgajiem vai uzņēmuma), kas tiek izmantoti komunikācijas izplatīšanai.

3. Mērķi

3.1 Novērst konfidenciālas, sensitīvas vai reglamentētas informācijas nejaušu vai tīšu izpaušanu ārējās komunikācijas kanālos.

3.2 Nodrošināt, ka oficiāli publiski paziņojumi un saturs sociālajos medijos ir precīzs, autorizēts un saskaņots ar uzņēmuma zīmola identitāti, ētikas principiem un stratēģisko komunikāciju.

3.3 Novērst reputācijas kaitējumu un nodrošināt konsekventu komunikāciju starp iekšējām struktūrvienībām un ārējām platformām.

3.4 Nodrošināt atbilstību piemērojamajiem tiesiskajiem pienākumiem attiecībā uz publiskiem paziņojumiem, tostarp VDAR, NIS2, DORA un nozarei specifiskiem komunikācijas noteikumiem.

3.5 Noteikt skaidrus pienākumus, pieļaujamos lietošanas gadījumus un politikas piemērošanas kārtību visam personālam, kas iesaistīts uz ārpusi vērstās aktivitātēs.

4. Lomas un pienākumi

4.1 Mārketinga vai komunikācijas vadītājs / sabiedrisko attiecību vadītājs

4.1.1 apstiprina visus oficiālos uzņēmuma paziņojumus publicēšanai ārpus organizācijas;

4.1.2 uztur sociālo mediju satura publicēšanas grafikus un vadlīnijas zīmola konsekvences nodrošināšanai;

4.1.3 uzrauga tiešsaistes pieminējumus un mediju atspoguļojumu, kas saistīts ar organizāciju.

4.2 Galvenais informācijas drošības vadītājs (CISO) / drošības komanda

4.2.1 uzrauga digitālās platformas, lai identificētu datu noplūžu, uzdošanās par citu personu vai pikšķerēšanas mēģinājumu indikatorus;

4.2.2 koordinē darbības ar incidentu reaģēšanas komandām sociālajos medijos balstītu uzbrukumu vai pārkāpumu gadījumā.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Ievērošana un atbilstība

9.1 Šī politika ir obligāta visam tās darbības jomā ietvertajam personālam un trešajām personām. Tās neievērošanas gadījumā var tikt piemērots:

9.1.1 formāls brīdinājums;

9.1.2 pagaidu vai pastāvīga piekļuves atsaukšana platformām vai sistēmām;

9.1.3 disciplinārpasākumi, tostarp darba attiecību izbeigšana;

9.1.4 tiesvedība, ja ārējā komunikācija izraisa reputācijas kaitējumu, datu aizsardzības pārkāpumu vai regulatīvo prasību neievērošanu.

9.2 Disciplinārās darbības

9.2.1 Iekšēji pārkāpumi (piemēram, konfidenciālu datu nopludināšana, organizācijas nomelnošana) izraisa Cilvēkresursu funkcijas (HR) iesaisti, formālu izmeklēšanu un dokumentēšanu darbinieka lietā.

9.2.2 Ja piemērojams, juridiskā funkcija ierosinās civiltiesiskās aizsardzības līdzekļus vai informēs iestādes par noziedzīgām darbībām (piemēram, uzdošanos par citu personu, iekšējās informācijas nopludināšanu tirdzniecības nolūkā).

9.3 Atbilstības uzraudzība

9.3.1 Drošības un komunikācijas komandām nepārtraukti jāveic uzraudzība attiecībā uz:

9.3.1.1 zīmola pieminējumiem galvenajās platformās;

9.3.1.2 neoficiālu uzņēmuma vizuālās identitātes vai preču zīmju izmantošanu;

9.3.1.3 zināmajiem riskiem (piemēram, neapmierinātiem darbiniekiem, uzdošanās par citu personu mēģinājumiem).

9.3.2 Uzraudzībai jāatbilst darbinieku privātuma tiesiskajām prasībām un normatīvajiem aktiem, un visi atzīmētie gadījumi jāpārbauda cilvēkam.

9.4 Trauksmes celšana un ziņošana par neatbilstošu lietošanu

9.4.1 Ikviens darbinieks, kuram ir aizdomas par šīs politikas pārkāpumu, tiek aicināts par to ziņot Informācijas drošības komandai, juridiskajai funkcijai vai anonīmi, izmantojot trauksmes celšanas portālu.

9.4.2 Jebkāda vēršanās pret trauksmes cēlējiem ir stingri aizliegta, un par to nekavējoties tiks piemērota disciplināra rīcība.

10. Pārskatīšanas un atjaunināšanas prasības

10.1 Šī politika jāpārskata reizi gadā vai agrāk, ja:

10.1.1 notiek būtiskas izmaiņas regulatīvajās prasībās (piemēram, jauni ES tiesību akti digitālās komunikācijas jomā);

10.1.2 tiek ieviestas jaunas sociālās platformas vai komunikācijas kanāli;

10.1.3 ir noticis būtisks incidents vai atkārtoti pārkāpumi, kas liecina par procesu nepilnībām;

10.1.4 ir notikušas strukturālas vai vadības izmaiņas sabiedrisko attiecību, juridiskajā vai drošības funkcijā.

10.2 Pārskatīšana kopīgi jāveic:

10.2.1 mārketinga / sabiedrisko attiecību vadītājam;

10.2.2 CISO vai drošības risku vadītājam;

10.2.3 juridiskās funkcijas un atbilstības speciālistiem.

10.3 Atjauninājumi jādokumentē politikas grozījumu reģistrā un jākomunicē, izmantojot iekšējos informētības kanālus. Ja tiek veiktas būtiskas izmaiņas, visam skartajam personālam atkārtoti jāapliecina politikas ievērošana.

11. Saistītās politikas un sasaiste

11.1 Šo politiku atbalsta un ar to ir savstarpēji saistītas šādas organizācijas informācijas drošības pārvaldības sistēmas (IDPS) sastāvdaļas:

11.1.1 P1 – Informācijas drošības politika: nosaka vispārējos principus informācijas aizsardzībai, tostarp nodrošina, ka komunikācija neizraisa nesankcionētu izpaušanu.

11.1.2 P3 – Pieļaujamās lietošanas politika: definē pieļaujamu rīcību digitālajās platformās un tehnoloģijās, kas tieši reglamentē sociālo kanālu personīgu un profesionālu lietošanu.

11.1.3 P6 – Risku pārvaldības politika: nosaka risku ietvaru, lai novērtētu ar publisko komunikāciju un reputācijas ietekmi saistītos apdraudējumus.

11.1.4 P8 – Informācijas drošības informētības un apmācību politika: nosaka informētības programmas, kas izglīto personālu par drošas komunikācijas praksi un sociālās inženierijas apdraudējumiem.

11.1.5 P13 – Datu klasifikācijas un marķēšanas politika: sniedz personālam norādes par to, kas uzskatāms par ierobežotas pieejamības vai konfidenciālu informāciju, kuru nedrīkst izpaust ārpus organizācijas.

11.1.6 P30 – Incidentu reaģēšanas politika: nosaka, kā rīkoties ar publisko komunikāciju saistītos incidentos, tostarp datu noplūžu, uzdošanās par citu personu un regulatīvo prasību pārkāpumu gadījumos.

11.1.7 P33 – Audita un atbilstības uzraudzības politika: reglamentē audita procesus, kas validē sociālo mediju kontroles pasākumus, uzraudzības sistēmas un atbilstību ārējās komunikācijas politikām.

12. Atsauces standarti un ietvari

12.1 ISO/IEC 27001:

12.1.1 8.1. punkts – darbības plānošana un kontrole: prasa noteiktus procesus un lomās balstītu pārvaldību publiskās komunikācijas pārvaldībai, nodrošinot precizitāti, apstiprināšanas darbplūsmas un ar datu vai reputācijas risku saistītu incidentu eskalāciju.

12.2 ISO/IEC 27002:2022:

12.2.1 5.10. kontrole – informācijas izmantošana: regulē autorizētu un ētisku iekšējās vai ārējās komunikācijas izplatīšanu.

12.2.2 5.11. kontrole – informācijas un aktīvu pieļaujamā lietošana: nostiprina pieļaujamo praksi satura kopīgošanai, izmantojot uzņēmuma aktīvus vai personīgos kontus.

12.2.3 5.35. kontrole – saziņa ar iestādēm: prasa strukturētu un autorizētu ārējo komunikāciju ar regulatīvajām iestādēm un publiskajām aģentūrām.

12.2.4 5.36. kontrole – atbilstība politikām un standartiem: nodrošina konsekventu iekšējo politiku piemērošanu visos komunikācijas scenārijos.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – uzvedības noteikumi: prasa formālus noteikumus sistēmu un komunikācijas izmantošanai, tostarp publiskas izpaušanas standartus.

12.3.2 AC-8 – sistēmas izmantošanas paziņojums: atbalsta obligātus atrunu tekstus un satura brīdinājumus ārēji pieejamās platformās.

12.3.3 AU-12 – audita ierakstu saglabāšana: attiecas uz žurnālu un komunikācijas vēstures saglabāšanu incidentu pārskatīšanai un audita vajadzībām.

12.4 ES VDAR (2016/679):

12.4.1 5. pants – datu apstrādes principi: aizliedz personas datu nesankcionētu kopīgošanu publiskā komunikācijā.

12.4.2 25. pants – datu aizsardzība pēc projektēšanas un pēc noklusējuma: prasa privātuma kontroles pasākumus komunikācijas rīkos un satura darbplūsmās.

12.4.3 32. pants – apstrādes drošība: attiecas uz šifrēšanu, piekļuves kontroli un satura apstiprināšanas procesiem.

12.4.4 33. pants – paziņošana par pārkāpumu: nosaka pienākumu savlaicīgi ziņot par personas datu noplūdēm publiskajos kanālos.

12.5 ES NIS2 direktīva (2022/2555):

12.5.1 21. pants – kiberdrošības risku pārvaldības pasākumi: ietver komunikācijas protokolus un pienākumus incidentu laikā, kā arī publiskajā komunikācijā par risku.

12.6 ES DORA (2022/2554):

12.6.1 9. pants – IKT risku pārvaldība: attiecas uz ārēji izraisītiem komunikācijas riskiem, piemēram, uzdošanos par citu personu, dezinformāciju un reputācijas traucējumiem.

12.6.2 16. pants – komunikācijas stratēģija: prasa, lai kritiski svarīgi finanšu vai pakalpojumu sniedzēji pārvaldītu komunikācijas riskus un reaģēšanu krīzes scenārijos.

12.7 COBIT 2019:

12.7.1 APO09 – pārvaldītas pakalpojumu vienošanās un komunikācija: prasa strukturētu pārvaldību iekšējai un ārējai komunikācijai.

12.7.2 DSS05 – drošības pakalpojumu pārvaldība: nodrošina, ka komunikācijas darbības nerada papildu risku un nepasliktina incidentu apstrādes procesus.