					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 standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5.1., 5.2., 6.1., 8. punkts	Vadība, riski un ārējās komunikācijas darbības kontroles pasākumi
ISO/IEC 27002:2022	5.10., 5.11. kontrole	Pieļaujamā lietošana un informācijas drošība komunikācijā
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Uzvedības noteikumi, audits, ziņošana par incidentiem un publiski pieejama satura un piekļuves pārvaldība
Vispārīgā datu aizsardzības regula (GDPR)	5., 32., 33. pants	Datu aizsardzības principi, apstrādes drošība un paziņošana par pārkāpumu, kas ietekmē publisko komunikāciju
NIS2 direktīva	21. panta 2. punkta e) un f) apakšpunkts	Politikas informācijas sistēmu izmantošanai un piegādes ķēdes un publiskās komunikācijas risku pārvaldībai
DORA regula	14. panta 4. punkts	Komunikācijas pienākumi pēc incidentiem

1. Mērķis

1.1. Šī politika nosaka obligātas prasības visai publiski pieejamai komunikācijai, tostarp sociālo mediju izmantošanai, saziņai ar presi un ārējam digitālajam saturam, ja tajā ir atsauce uz uzņēmumu, tā personālu, klientiem, sistēmām vai iekšējo praksi.

1.2. Politikas mērķis ir aizsargāt uzņēmuma reputāciju, nodrošināt atbilstību tiesību aktu un regulatīvajām prasībām un mazināt datu noplūdes, dezinformācijas vai drošības incidentu risku.

1.3. Tā ļauj darbiniekiem un partneriem pozitīvi un atbildīgi iesaistīties tiešsaistes diskusijās, vienlaikus novēršot nejaušu informācijas izpaušanu vai maldinoša priekšstata radīšanu.

1.4. Politika stiprina SME gatavību ISO/IEC 27001 sertifikācijai, nosakot kontroles pasākumus pār informāciju, kas tiek padarīta pieejama sabiedrībai vai ārējām ieinteresētajām pusēm.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visām ar organizāciju saistītajām personām, tostarp:

2.1.1. darbiniekiem un līgumslēdzējiem;

2.1.2. ārštata speciālistiem, konsultantiem un trešo pušu piegādātājiem;

2.1.3. praktikantiem vai nepilna laika darbiniekiem, kuri iesaistīti klientu apkalpošanā vai kuriem ir piekļuve sistēmām.

2.2. Politika attiecas uz visām ārējās komunikācijas formām, kurās ir atsauce uz organizāciju, tostarp:

2.2.1. ierakstiem sociālajos medijos (LinkedIn, X, TikTok, Instagram, Facebook u. c.);

2.2.2. emuāru ierakstiem, tiešsaistes forumiem, klientu atsauksmēm un diskusiju pavedieniem;

2.2.3. publiskām uzstāšanām (piemēram, konferencēs, tīmekļsemināros, podkāstos);

2.2.4. e-pastiem vai ziņojumiem žurnālistiem, valsts iestāžu pārstāvjiem vai ietekmes veidotājiem;

2.2.5. publiski kopīgotiem ekrānattēliem, fotogrāfijām vai video no darba vides.

2.3. Politika ir piemērojama arī tad, ja šāda komunikācija tiek veikta:

2.3.1. no personīgām ierīcēm vai kontiem;

2.3.2. ārpus parastā darba laika;

2.3.3. bez ļaunprātīga nolūka — arī nejaušas vai garāmejot izteiktas piezīmes ietilpst šīs politikas tvērumā, ja tās attiecas uz uzņēmumu.

3. Mērķi

3.1. Reputācijas aizsardzība: novērst kaitējumu uzņēmuma reputācijai, ko rada nesankcionēta vai neatbilstoša publiskā komunikācija.

3.2. Datu drošība: nepieļaut sensitīvu datu, iekšējo sistēmu vai klientu informācijas nejaušu izpaušanu sociālajos medijos vai publiskos kanālos.

3.3. Atbilstība tiesību aktu un regulatīvajām prasībām: nodrošināt, lai viss publiskais saturs ar atsauci uz uzņēmumu atbilstu piemērojamajiem datu aizsardzības un komercsaziņas normatīvajiem aktiem.

3.4. Profesionāla rīcība: nodrošināt atbildīgu līdzdalību tiešsaistes diskusijās un saziņā ar medijiem arī personīgajos kontos.

3.5. Gatavība incidentiem: noteikt skaidras un izpildāmas darbības nejaušas informācijas izpaušanas vai politikas pārkāpumu gadījumā.

4. Lomas un pienākumi

4.1. Ģenerāldirektors (GM)

4.1.1. ir šīs politikas īpašnieks un apstiprinātājs;

4.1.2. pārskata un apstiprina jebkurus publiski pieejamus paziņojumus, saziņu ar presi vai intervijas medijiem;

4.1.3. nodrošina, ka šī politika tiek skaidri komunicēta visiem darbiniekiem un trešajām pusēm;

4.1.4. sadarbībā ar incidentu reaģēšanas procedūrām izmeklē un risina jebkurus šīs politikas pārkāpumus.

4.2. Norīkotais darbinieks vai komunikācijas vadītājs (ja tāds ir norīkots)

4.2.1. atbalsta GM, pārskatot saturu pirms tā ārējas publicēšanas (piemēram, emuāru ierakstus, uzstāšanās tēmas);

4.2.2. uztur apstiprināto mediju aktivitāšu vai augsta riska ierakstu sociālajos medijos žurnālus;

4.2.3. atbilstoši pieejamajai kapacitātei uzrauga zināmās atsauces uz uzņēmumu tiešsaistē, lai identificētu reputācijas vai drošības riskus.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Ikgadējā pārskatīšana

9.1.1. Šī politika jāpārskata vismaz reizi gadā ģenerāldirektoram (GM).

9.1.2. Pārskatīšanā jānodrošina atbilstība aktualizētajām tiesību aktu prasībām, nozares komunikācijas tendencēm un iekšējām uzņēmējdarbības izmaiņām.

9.2. Pārskatīšana pēc ierosinātājiem

9.2.1. Šī politika nekavējoties jāatjaunina pēc:

9.2.1.1. būtiska incidenta sociālajos medijos vai reputācijas problēmas;

9.2.1.2. izmaiņām trešo pušu piegādātājos, kas pārvalda komunikāciju;

9.2.1.3. jauna tiesiskā regulējuma vai regulatīvo pienākumu noteikšanas attiecībā uz tiešsaistes komunikāciju, medijiem vai zīmola lietojumu.

9.3. Izmaiņu dokumentēšana

9.3.1. Jāreģistrē visi atjauninājumi, tostarp pārskatīšanas datums, izmaiņu kopsavilkums un GM apstiprinājums.

9.3.2. Audita un sertifikācijas vajadzībām jāuztur versiju vēsture.

9.4. Atjauninājumu izplatīšana

9.4.1. Visi darbinieki un līgumslēdzēji jāinformē par jebkuriem politikas grozījumiem.

9.4.2. Atjauninātās versijas jāizplata e-pastā vai iekšējos portālos.

9.4.3. Jebkuram publiskās komunikācijas piegādātājam pirms darba turpināšanas jāapliecina aktualizēto noteikumu pieņemšana.

10. Saistītās politikas un sasaiste

10.1. Šī politika darbojas sasaistē ar šādām SME politikām:

10.1.1. P3S – Pieļaujamās lietošanas politika (AUP): nosaka pieņemamu rīcību, izmantojot saziņas platformas, tostarp piekļuvi sociālajiem medijiem darba laikā.

10.1.2. P8S – Informācijas drošības informētības un apmācības politika: nodrošina, ka personāls ir apmācīts atpazīt pārmērīgas informācijas atklāšanas, pikšķerēšanas vai reputācijas apdraudējumu riskus tiešsaistē.

10.1.3. P17S – Datu aizsardzības un privātuma politika: nodrošina, ka personas dati un klientu dati netiek kopīgoti ārējā komunikācijā, ievērojot GDPR un citas tiesību aktu prasības.

10.1.4. P30S – Incidentu reaģēšanas politika: nosaka reaģēšanu uz nejaušu publisku informācijas izpaušanu, tiešsaistes apdraudējumiem vai reputācijas uzbrukumiem, kas radušies sociālo mediju neatbilstošas lietošanas dēļ.

10.1.5. P37S – Juridiskās un regulatīvās atbilstības politika: nosaka organizācijas plašākos tiesiskos un līgumiskos pienākumus, publiski kopīgojot saturu.

10.2. Šīs politikas jāpiemēro kopā, lai uzturētu drošu, cieņpilnu un tiesību aktiem atbilstošu ārējo klātbūtni.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 5.1. punkts – vadība un apņemšanās: nosaka vadības pārraudzību pār reputācijas un informācijas riskiem.

11.1.2. 6.1. punkts – risku pārvaldība: ietver ar komunikāciju saistītu pakļautību riskam.

11.1.3. 8.1. punkts – darbības kontrole: aptver noteikumus tam, kā informācija tiek komunicēta ārēji.

11.2. ISO/IEC 27002

11.2.1. 5.10. kontrole – informācijas un aktīvu pieļaujamā lietošana.

11.2.2. 5.11. kontrole – informācijas drošība komunikācijā.

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – uzvedības noteikumi: nosaka atbilstošu rīcību, izmantojot informācijas resursus.

11.3.2. AU-7 – audita apjoma samazināšana un pārskatu ģenerēšana: atbalsta publisku sistēmu izmantošanas uzraudzību.

11.3.3. IR-6 – ziņošana par incidentiem: nosaka reaģēšanu uz reputācijas un komunikācijas pārkāpumiem.

11.3.4. AC-22 – publiski pieejams saturs: nodrošina kontroli pār ārējām publikācijām un piekļuvi tām.

11.4. GDPR (Regula (ES) 2016/679)

11.4.1. 5. pants – principi attiecībā uz personas datu apstrādi (precizitāte, integritāte, pārskatatbildība).

11.4.2. 32. pants – apstrādes drošība: nosaka drošības pasākumus publiskai kopīgošanai.

11.4.3. 33. pants – paziņošana par personas datu aizsardzības pārkāpumu: piemērojama, ja personas dati tiek izpausti ārējā komunikācijā.

11.5. NIS2 direktīva (Direktīva (ES) 2022/2555)

11.5.1. 21. panta 2. punkta e) apakšpunkts – politikas par informācijas sistēmu izmantošanu, tostarp komunikācijas platformām.

11.5.2. 21. panta 2. punkta f) apakšpunkts – politikas kiberdrošības risku pārvaldībai piegādes ķēdē un publiskajās platformās.

11.6. DORA regula (Regula (ES) 2022/2554)

11.6.1. 14. panta 4. punkts – komunikācijas pienākumi pret klientiem, trešajām pusēm un iestādēm pēc darbības incidentiem.

11.7. COBIT 2019

11.7.1. APO09 – pakalpojumu līmeņa vienošanos (SLA) pārvaldība: aptver piegādātāju un ar komunikāciju saistītu trešo pušu pārraudzību.

11.7.2. DSS05 – drošības pakalpojumu pārvaldība: ietver publiski pieejamu digitālo aktīvu aizsardzību.

11.7.3. EDM03 – riska optimizācijas nodrošināšana: uzsver ar komunikāciju saistītu reputācijas un atbilstības risku pārvaldību.