					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P36S					Dokumendi pealkiri: **Sotsiaalmeedia ja väliskommunikatsiooni poliitika**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.1, 5.2, 6.1, 8	juhtimine, riskijuhtimine ning väliskommunikatsiooni tegevuste planeerimine ja ohje
ISO/IEC 27002:2022	Kontrollimeetmed 5.10, 5.11	lubatud kasutus ja infoturve teabevahetuses
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	käitumisreeglid, audit, intsidentidest teatamine ning avaliku sisu ja juurdepääsu haldus
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5, 32, 33	andmekaitse põhimõtted, töötlemise turvalisus ja isikuandmete rikkumisest teavitamine, mis mõjutab avalikku kommunikatsiooni
ELi NIS2	Artikkel 21(2)(e), 21(2)(f)	infosüsteemide kasutamise poliitikad ning tarneahela ja avaliku kommunikatsiooni riskide juhtimine
ELi DORA	Artikkel 14(4)	tegevusintsidentide järel kohalduvad teabevahetuskohustused

1. Eesmärk

1.1. Käesolev poliitika kehtestab kohustuslikud nõuded kogu avalikkusele suunatud kommunikatsioonile, sealhulgas sotsiaalmeedia kasutamisele, meediasuhtlusele ja välisele digitaalsele sisule, kui viidatakse ettevõttele, selle töötajatele, klientidele, süsteemidele või sisemistele tööpraktikatele.

1.2. Poliitika eesmärk on kaitsta ettevõtte mainet, tagada vastavus õigus- ja regulatiivsetele nõuetele ning vähendada teabelekete, väärinfo ja turbeintsidentide riski.

1.3. Poliitika aitab töötajatel ja partneritel osaleda veebiaruteludes positiivselt ja vastutustundlikult, vältides samal ajal juhuslikku teabe avaldamist või eksitava mulje jätmist.

1.4. Poliitika toetab VKE valmisolekut ISO/IEC 27001 sertifitseerimiseks, käsitledes avalikkusele või välistele sidusrühmadele kättesaadavaks tehtava teabe kontrolli.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigile organisatsiooniga seotud isikutele, sealhulgas:

2.1.1. töötajatele ja töövõtjatele

2.1.2. vabakutselistele, konsultantidele ja kolmandatest isikutest tarnijatele

2.1.3. praktikantidele või osalise tööajaga töötajatele, kes osalevad klienditeeninduses või kellel on juurdepääs süsteemidele

2.2. Poliitika kehtib kõigile organisatsioonile viitavatele väliskommunikatsiooni vormidele, sealhulgas:

2.2.1. sotsiaalmeediapostitustele (LinkedIn, X, TikTok, Instagram, Facebook jne)

2.2.2. blogipostitustele, veebifoorumitele, kliendiarvustustele ja arutelulõimedele

2.2.3. esinemistele (nt konverentsid, veebiseminarid, taskuhäälingud)

2.2.4. e-kirjadele või sõnumitele ajakirjanikele, riigiasutuste esindajatele või mõjuisikutele

2.2.5. avalikult jagatud ekraanipiltidele, fotodele või videotele töökeskkonnast

2.3. Poliitika kehtib ka juhul, kui selline kommunikatsioon toimub:

2.3.1. isiklikest seadmetest või kontodelt

2.3.2. väljaspool tavapärast tööaega

2.3.3. pahatahtliku kavatsuseta — ka juhuslikud või möödaminnes tehtud märkused kuuluvad poliitika kohaldamisalasse, kui need viitavad ettevõttele

3. Eesmärgid

3.1. Maine kaitse: vältida ettevõtte maine kahjustamist volitamata või sobimatu avaliku kommunikatsiooni kaudu

3.2. Andmeturve: vältida tundlike andmete, sisemiste süsteemide või kliendiandmete tahtmatut avalikustamist sotsiaalmeedias või avalikes kanalites

3.3. Vastavus õigus- ja regulatiivsetele nõuetele: tagada, et kogu ettevõttele viitav avalik sisu vastab asjakohastele andmekaitse- ja ärikommunikatsiooni nõuetele

3.4. Professionaalne käitumine: soodustada vastutustundlikku osalemist veebiaruteludes ja meediasuhtluses, sealhulgas isiklike kontode kasutamisel

3.5. Intsidentideks valmisolek: kehtestada selged ja rakendatavad tegevused juhuks, kui toimub juhuslik avalikustamine või poliitika rikkumine

4. Rollid ja vastutused

4.1. tegevjuht

4.1.1. vastutab poliitika eest ja kinnitab selle

4.1.2. vaatab läbi ja annab loa kõigile avalikkusele suunatud seisukohtadele, meediasuhtlusele või meediaintervjuudele

4.1.3. tagab, et poliitika on selgelt edastatud kõigile töötajatele ja kolmandatele isikutele

4.1.4. uurib kõiki käesoleva poliitika rikkumisi ja reageerib neile kooskõlas intsidentide halduse protseduuridega

4.2. määratud töötaja või kommunikatsiooni eest vastutav isik (kui see on määratud)

4.2.1. toetab tegevjuhti, vaadates enne välist avaldamist läbi sisu, näiteks blogipostitused või esinemiste teemad

4.2.2. peab arvestust heakskiidetud meediategevuste või kõrgema riskiga sotsiaalmeediapostituste üle

4.2.3. jälgib võimaluste piires ettevõtte teadaolevaid mainimisi veebis maine- või turberiskide tuvastamiseks

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Iga-aastane läbivaatamine

9.1.1. Käesoleva poliitika peab vähemalt kord aastas läbi vaatama tegevjuht

9.1.2. Läbivaatamisel tuleb tagada kooskõla ajakohastatud õiguslike kohustuste, valdkonna kommunikatsioonitrendide ja ettevõttesiseste ärimuudatustega

9.2. Sündmuspõhised läbivaatamised

9.2.1. Käesolevat poliitikat tuleb viivitamata ajakohastada pärast järgmist:

9.2.1.1. olulist sotsiaalmeediaintsidenti või maineprobleemi

9.2.1.2. kommunikatsiooni haldavate kolmandatest isikutest tarnijate muutust

9.2.1.3. uut õigusakti või regulatiivset kohustust, mis puudutab veebikommunikatsiooni, meediat või kaubamärki

9.3. Muudatuste dokumenteerimine

9.3.1. Kõik ajakohastused tuleb registreerida, sealhulgas läbivaatamise kuupäev, muudatuste kokkuvõte ja tegevjuhi heakskiit

9.3.2. Auditi ja sertifitseerimise eesmärgil tuleb säilitada versiooniajalugu

9.4. Ajakohastuste jagamine

9.4.1. Kõiki töötajaid ja töövõtjaid tuleb teavitada poliitikamuudatustest

9.4.2. Ajakohastatud versioonid tuleb jagada e-posti või sisemiste portaalide kaudu

9.4.3. Iga avaliku kommunikatsiooni teenuseosutaja peab enne töö jätkamist kinnitama ajakohastatud tingimustega tutvumist

10. Seotud poliitikad ja seosed

10.1. Käesolevat poliitikat rakendatakse koostoimes järgmiste VKE poliitikatega:

10.1.1. P3S – IT-vahendite lubatud kasutuse poliitika: määratleb lubatud käitumise kommunikatsiooniplatvormide kasutamisel, sealhulgas sotsiaalmeedia kasutamisel tööajal

10.1.2. P8S – infoturbeteadlikkuse ja koolituse poliitika: tagab, et töötajad on koolitatud ära tundma ülemäärase jagamise, andmepüügi või veebikeskkonnas esinevate maineohtude riske

10.1.3. P17S – andmekaitse ja privaatsuspoliitika: tagab, et isikuandmeid ja kliendiandmeid ei jagata väliskommunikatsioonis ning et tegevus on kooskõlas GDPR-i ja muude õiguslike nõuetega

10.1.4. P30S – Intsidentidele reageerimise poliitika: reguleerib reageerimist juhuslikule avalikule avalikustamisele, veebiohtudele või mainekahjule, mis tuleneb sotsiaalmeedia väärkasutusest

10.1.5. P37S – õigusliku ja regulatiivse vastavuse poliitika: määratleb organisatsiooni laiemad õiguslikud ja lepingulised kohustused avaliku sisu jagamisel

10.2. Neid poliitikaid tuleb rakendada koos, et tagada turvaline, lugupidav ja õigusnõuetele vastav väline kohalolu.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 5.1 – juhtimine ja pühendumus: nõuab juhtkonna järelevalvet maine- ja teaberiskide üle

11.1.2. Punkt 6.1 – riskijuhtimine: hõlmab kommunikatsiooniga seotud riskipositsioone

11.1.3. Punkt 8.1 – tegevuse planeerimine ja ohje: hõlmab reegleid selle kohta, kuidas teavet väliselt edastatakse

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.10 – teabe ja varade lubatud kasutus

11.2.2. Kontroll 5.11 – infoturve teabevahetuses

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – käitumisreeglid: reguleerib asjakohast käitumist teabevarade kasutamisel

11.3.2. AU-7 – auditiandmete vähendamine ja aruannete koostamine: toetab avalike süsteemide kasutuse seiret

11.3.3. IR-6 – intsidentidest teatamine: nõuab reageerimist maine- ja kommunikatsioonirikkumistele

11.3.4. AC-22 – avalikult kättesaadav sisu: tagab kontrolli väliste avalduste ja juurdepääsu üle

11.4. ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.4.1. Artikkel 5 – isikuandmete töötlemise põhimõtted (täpsus, terviklus, vastutus)

11.4.2. Artikkel 32 – töötlemise turvalisus: nõuab kaitsemeetmeid avaliku jagamise korral

11.4.3. Artikkel 33 – rikkumisest teavitamine: kohaldub juhul, kui isikuandmed avalikustatakse väliskommunikatsiooni kaudu

11.5. ELi NIS2 direktiiv (2022/2555)

11.5.1. Artikkel 21(2)(e) – infosüsteemide kasutamise poliitikad, sealhulgas kommunikatsiooniplatvormid

11.5.2. Artikkel 21(2)(f) – poliitikad küberturberiskide käsitlemiseks tarneahelas ja avalikel platvormidel

11.6. ELi DORA määrus (2022/2554)

11.6.1. Artikkel 14(4) – teabevahetuskohustused klientide, kolmandate isikute ja asutustega pärast tegevusintsidente

11.7. COBIT 2019

11.7.1. APO09 – teenuslepingute haldus: hõlmab järelevalvet tarnijate ja kommunikatsiooniga seotud kolmandate isikute üle

11.7.2. DSS05 – turbeteenuste haldus: hõlmab avalikkusele suunatud digitaalsete varade kaitset

11.7.3. EDM03 – riskide optimeerimise tagamine: rõhutab kommunikatsiooniga seotud maine- ja vastavusriskide juhtimist