| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | |
| Dokumendi number:<br>P36 | | | | | Dokumendi pealkiri:<br>**Sotsiaalmeedia ja väliskommunikatsiooni poliitika** | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>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 õigusnormidega

| Standard/õigusnorm | Punkt/artikkel | Kommentaar |
|---|---|---|
| ISO/IEC 27001:2022 | Punkt 8 | Määratletud protsessid ja rollipõhine juhtimine avaliku suhtluse haldamiseks, tagades täpsuse, kooskõlastamise töövood ja intsidentide eskaleerimise. |
| ISO/IEC 27002:2022 | Kontrollimeetmed 5.10, 5.11, 5.35, 5.36 | Reguleerib kasutust, ettevõtte varade lubatud kasutust, väliskontakte ja suhtlust asutustega ning vastavuse aruandlust. |
| NIST SP 800-53 Rev.5 | AC-8, AU-12, PL-4 | Süsteemide ja suhtlusvahendite kasutamise reeglid, kasutajate teavitused ning auditilogide säilitamine. |
| ELi isikuandmete kaitse üldmäärus (GDPR) | Artiklid 5, 25, 32, 33 | Andmetöötluse põhimõtted, lõimitud ja vaikimisi andmekaitse, töötlemise turvalisus ning rikkumisest teatamise nõuded. |
| ELi NIS2 direktiiv | Artikkel 21 | Küberturbe riskijuhtimise meetmed, kohustused intsidentide korral ning riskidega seotud avalik teabevahetus. |
| ELi DORA määrus | Artiklid 9, 16 | IKT-riski juhtimine ja suhtlusstrateegia kriitiliste teenuseosutajate jaoks. |
| COBIT 2019 | APO09, DSS05 | Teenuslepingute ja suhtluse juhtimine ning turvalise suhtluse praktikad / intsidendihaldus. |

**1. Eesmärk**

1.1 Käesolev poliitika kehtestab kohustuslikud reeglid ja vastutused, mis reguleerivad sotsiaalmeedia ja kõigi välissuhtluse vormide kasutamist organisatsiooniga seotud isikute poolt.

1.2 Sellega tagatakse, et avalik suhtlus — olenemata sellest, kas see on planeeritud või spontaanne — on täpne, lugupidav, turvaline, õigusnormidele vastav ja kooskõlas organisatsiooni brändikasutuse põhimõtetega.

1.3 Poliitika eesmärk on minimeerida riske, mis on seotud mainekahju, õigusnormide rikkumise, intellektuaalomandi lekkimise ja loata avalikustamisega avalike kanalite kaudu.

1.4 Samuti edendab see vastutust ja struktureeritud juhtimist kõigis digitaalse suhtluse vormides, mis hõlmavad organisatsiooni või mõjutavad seda.

**2. Kohaldamisala**

**2.1 Käesolev poliitika kehtib kõigile töötajatele, töövõtjatele, praktikantidele ja kolmandate osapoolte esindajatele, kes:**

2.1.1 suhtlevad organisatsiooni nimel, ametlikult või mitteametlikult;

2.1.2 viitavad avalikus keskkonnas organisatsiooniga seotusele või annavad sellest mõista;

2.1.3 kasutavad isiklikke või ettevõtte kontosid, et osaleda organisatsiooniga seotud avalikes aruteludes.

**2.2 Hõlmatud suhtluskanalid hõlmavad muu hulgas järgmist:**

2.2.1 sotsiaalmeediaplatvormid (nt LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook);

2.2.2 blogid, vikid, foorumid ja avalikud arutelutahvlid;

2.2.3 e-post või otsesõnumid välistele osapooltele (nt kliendid, regulaatorid, meedia);

2.2.4 pressiintervjuud, paneelarutelud või salvestatud meediaesinemised;

2.2.5 osalemine veebikogukondades, kus organisatsioonile viidatakse.

2.3 Käesolev poliitika reguleerib nii reaalajas kui ka ette ajastatud sisu ning kehtib kõigile seadmetele ja kontodele (isiklikud või ettevõtte omad), mida kasutatakse sellise suhtluse levitamiseks.

**3. Eesmärgid**

3.1 Vältida konfidentsiaalse, tundliku või reguleeritud teabe juhuslikku või tahtlikku avalikustamist väliste suhtluskanalite kaudu.

3.2 Tagada, et ametlikud avalikud avaldused ja sotsiaalmeediasisu on täpsed, volitatud ning kooskõlas ettevõtte brändi, eetika ja strateegiliste sõnumitega.

3.3 Ennetada mainekahju ja tagada sõnumite järjepidevus organisatsiooni siseste üksuste ja väliste platvormide vahel.

3.4 Täita avalike avaldustega seotud kohaldatavaid õiguslikke kohustusi, sealhulgas GDPRi, NIS2, DORA ja valdkonnaspetsiifiliste suhtlusreeglite nõudeid.

3.5 Määratleda selged vastutused, lubatud kasutusjuhud ja rakendusprotokollid kõigile töötajatele, kes osalevad avalikkusele suunatud tegevustes.

**4. Rollid ja vastutused**

**4.1 Turundusjuht, kommunikatsioonijuht või PR-juht**

4.1.1 Kiidab heaks kogu ametliku ettevõtte suhtluse väliseks avaldamiseks.

4.1.2 Haldab sotsiaalmeedia sisukalendreid ja suuniseid brändi järjepidevuse tagamiseks.

4.1.3 Seirab organisatsiooniga seotud veebimainimisi ja meediakajastust.

**4.2 Infoturbe juht või turvameeskond**

4.2.1 Seirab digiplatvorme andmelekkega, kehastamisega või andmepüügikatsetega seotud indikaatorite tuvastamiseks.

4.2.2 Koordineerib koostööd intsidentidele reageerimise meeskondadega sotsiaalmeediapõhiste rünnakute või rikkumiste korral.

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

**9. Rakendamine ja vastavus**

**9.1 Käesolev poliitika on kohustuslik kõigile hõlmatud töötajatele ja kolmandatele osapooltele. Nõuete eiramine võib kaasa tuua:**

9.1.1 ametlikud kirjalikud hoiatused;

9.1.2 ajutise või püsiva juurdepääsuõiguste tühistamise platvormidele või süsteemidele;

9.1.3 distsiplinaarmeetmed, sealhulgas töösuhte lõpetamise;

9.1.4 kohtumenetluse, kui välissuhtlus põhjustab mainekahju, andmekaitserikkumise või õigusnormidele mittevastavuse.

**9.2 Distsiplinaarmeetmed**

9.2.1 Sisemised rikkumised (nt konfidentsiaalsete andmete lekitamine, organisatsiooni laimamine) toovad kaasa personali (HR) kaasamise, ametliku uurimise ja dokumenteerimise töötaja toimikus.

9.2.2 Kui see on asjakohane, kasutab õigusfunktsioon tsiviilõiguslikke õiguskaitsevahendeid või teavitab ametiasutusi kuritegelikust tegevusest (nt kehastamine, siseinfo lekked kauplemise eesmärgil).

**9.3 Vastavuse seire**

**9.3.1 Turva- ja kommunikatsioonimeeskonnad peavad tegema pidevat seiret järgmise üle:**

9.3.1.1 brändimainimised peamistel platvormidel;

9.3.1.2 ettevõtte kujutiste või kaubamärkide mitteametlik kasutamine;

9.3.1.3 teadaolevad riskid (nt rahulolematud töötajad, kehastamiskatsed).

9.3.2 Seire peab vastama töötajate andmekaitset käsitlevatele seadustele ja regulatsioonidele ning kõik märgistatud juhtumid peab üle kontrollima inimene.

**9.4 Rikkumisest teavitamine ja väärkasutuse raporteerimine**

9.4.1 Iga töötajat, kes kahtlustab käesoleva poliitika rikkumist, julgustatakse sellest teatama infoturbe meeskonnale, õigusfunktsioonile või anonüümselt rikkumisest teavitamise portaali kaudu.

9.4.2 Survemeetmed teavitajate suhtes on rangelt keelatud ja toovad kaasa viivitamatud distsiplinaarmeetmed.

**10. Läbivaatamise ja ajakohastamise nõuded**

**10.1 Käesolev poliitika tuleb läbi vaadata kord aastas või varem, kui:**

10.1.1 regulatiivsetes nõuetes toimuvad olulised muudatused (nt uued ELi digitaalse suhtluse õigusaktid);

10.1.2 võetakse kasutusele uued sotsiaalplatvormid või suhtluskanalid;

10.1.3 toimub oluline intsident või korduvad rikkumised, mis viitavad protsessilünkadele;

10.1.4 toimuvad struktuurilised või juhtimistasandi muudatused PR-, õigus- või turbefunktsioonides.

**10.2 Läbivaatamise peavad ühiselt läbi viima:**

10.2.1 turundus- või PR-juht;

10.2.2 infoturbe juht või infoturberiskide juht;

10.2.3 õigus- ja vastavusametnikud.

10.3 Muudatused tuleb dokumenteerida poliitikamuudatuste registris ja edastada sisemiste teadlikkuse tõstmise kanalite kaudu. Oluliste muudatuste korral peavad kõik mõjutatud töötajad uuesti kinnitama poliitikaga tutvumist.

**11. Seotud poliitikad ja seosed**

**11.1 Käesolevat poliitikat toetavad ja sellega on seotud järgmised organisatsiooni infoturbe juhtimissüsteemi (ISMS) komponendid:**

11.1.1 P1 – Infoturbepoliitika: kehtestab üldpõhimõtted teabe kaitsmiseks, sealhulgas nõude, et suhtlus ei tohi viia loata avalikustamiseni.

11.1.2 P3 – IT-vahendite lubatud kasutuse poliitika: määratleb lubatud käitumise digiplatvormide ja tehnoloogiate kasutamisel, mis reguleerib otseselt sotsiaalsete kanalite isiklikku ja tööalast kasutamist.

11.1.3 P6 – Riskijuhtimise poliitika: annab riskiraamistiku avaliku suhtluse ja mainekahjuga seotud ohtude hindamiseks.

11.1.4 P8 – Infoturbeteadlikkuse koolituse poliitika: kehtestab teadlikkuse tõstmise programmid, mis õpetavad töötajatele turvalise suhtluse tavasid ja sotsiaalse manipuleerimise ohte.

11.1.5 P13 – Andmete klassifitseerimise ja märgistamise poliitika: juhendab töötajaid selles, mida käsitatakse piiratud või konfidentsiaalse teabena, mida ei tohi väliselt avaldada.

11.1.6 P30 – Intsidentidele reageerimise poliitika: määratleb, kuidas käsitleda avaliku suhtlusega seotud intsidente, sealhulgas andmelekked, kehastamine ja õigusnormide rikkumine.

11.1.7 P33 – Auditi ja nõuetele vastavuse seire poliitika: reguleerib auditiprotsesse, millega valideeritakse sotsiaalmeedia kontrollimeetmeid, seiresüsteeme ja vastavust välissuhtluse poliitikatele.

## 12. Viitestandardid ja raamistikud

### 12.1 ISO/IEC 27001:

12.1.1 Punkt 8.1 – Tegevuse planeerimine ja ohje: nõuab määratletud protsesse ja rollipõhist juhtimist avaliku suhtluse haldamiseks, tagades täpsuse, kooskõlastamise töövood ning andmete või mainega seotud riskiga intsidentide eskaleerimise.

### 12.2 ISO/IEC 27002:2022:

12.2.1 Kontroll 5.10 – Teabe kasutamine: reguleerib sise- või välissuhtluse volitatud ja eetilist levitamist.

12.2.2 Kontroll 5.11 – Teabe ja varade lubatud kasutus: tugevdab lubatud kasutuse tavasid sisu jagamisel ettevõtte varade või isiklike kontode kaudu.

12.2.3 Kontroll 5.35 – Kontakt asutustega: nõuab struktureeritud ja volitatud välissuhtlust regulatiivsete asutuste ja avaliku sektori organisatsioonidega.

12.2.4 Kontroll 5.36 – Vastavus poliitikatele ja standarditele: nõuab sisepoliitikate järjepidevat rakendamist kõigis suhtlusolukordades.

### 12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Käitumisreeglid: nõuab ametlikke reegleid süsteemide ja suhtlusvahendite kasutamiseks, sealhulgas avalikustamise standardeid.

12.3.2 AC-8 – Süsteemi kasutamise teavitus: toetab kohustuslike lahtiütluste ja sisuteavituste kasutamist välistele osapooltele suunatud platvormidel.

12.3.3 AU-12 – Auditikirjete säilitamine: kohaldub logide ja suhtlusajaloo säilitamisele intsidendi läbivaatamise ja auditi eesmärgil.

### 12.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679):

12.4.1 Artikkel 5 – Andmetöötluse põhimõtted: keelab isikuandmete loata jagamise avaliku suhtluse kaudu.

12.4.2 Artikkel 25 – Lõimitud andmekaitse ja vaikimisi andmekaitse: nõuab andmekaitsemeetmete rakendamist suhtlusvahendites ja sisu töövoogudes.

12.4.3 Artikkel 32 – Töötlemise turvalisus: hõlmab krüpteerimist, juurdepääsukontrolli ja sisu kooskõlastamise protsesse.

12.4.4 Artikkel 33 – Rikkumisest teavitamine: nõuab isikuandmete rikkumiste õigeaegset teatamist avalike kanalite kaudu.

### 12.5 ELi NIS2 direktiiv (2022/2555):

12.5.1 Artikkel 21 – Küberturbe riskijuhtimise meetmed: hõlmab suhtlusprotokolle ja kohustusi intsidentide ajal ning riskidega seotud avalikus suhtluses.

### 12.6 ELi DORA määrus (2022/2554):

12.6.1 Artikkel 9 – IKT-riski juhtimine: kohaldub väliselt käivitunud suhtlusriskidele, nagu kehastamine, valeinfo ja mainekahju põhjustavad häiringud.

12.6.2 Artikkel 16 – Suhtlusstrateegia: nõuab, et kriitilised finantsasutused või teenuseosutajad haldaksid suhtlusriske ja reageerimist kriisiolukordades.

### 12.7 COBIT 2019:

12.7.1 APO09 – Hallatud teenuslepingud ja suhtlus: nõuab struktureeritud juhtimist sise- ja välissuhtluse üle.

12.7.2 DSS05 – Turvateenuste haldamine: tagab, et suhtlustegevused ei too kaasa täiendavat riski ega kahjusta intsidentide käsitlemise protsesse.