					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P36S					Dokumento pavadinimas: **Socialinių tinklų ir išorinės komunikacijos politika**						
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:						
X	Politika		Standartas		Procedūra		Forma		Registras		Kita

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	Apibrėžti procesai ir vaidmenimis grindžiama valdysena, skirta viešosios komunikacijos valdymui, užtikrinant tikslumą, tvirtinimo eigą ir incidentų eskalavimą.
ISO/IEC 27002:2022	Kontrolės priemonės 5.10, 5.11, 5.35, 5.36	Reglamentuoja naudojimą, priimtiną organizacijos turto naudojimą, komunikaciją su išorės kontaktais ir institucijomis bei atitikties ataskaitų teikimą.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Sistemų ir komunikacijos naudojimo taisyklės, naudotojų pranešimai, audito įrašų saugojimas.
ES BDAR	5, 25, 32, 33 straipsniai	Duomenų tvarkymo principai, privatumas pagal projektavimą, tvarkymo saugumas, pranešimo apie pažeidimą reikalavimai.
ES NIS2 direktyva	21 straipsnis	Kibernetinio saugumo rizikos valdymo priemonės, pareigos incidentų atveju ir su rizika susijusi viešoji komunikacija.
ES DORA reglamentas	9, 16 straipsniai	IRT rizikos valdymas ir komunikacijos strategija kritinių paslaugų teikėjams.
COBIT 2019	APO09, DSS05	Paslaugų susitarimų ir komunikacijos valdysena bei saugios komunikacijos praktika / incidentų valdymas.

1. Tikslas

1.1 Ši politika nustato privalomas taisykles ir atsakomybes, reglamentuojančias socialinių tinklų naudojimą ir visas išorinės komunikacijos formas, kurias vykdo su organizacija susiję asmenys.

1.2 Ji užtikrina, kad viešoji komunikacija – planuota ar spontaniška – būtų tiksli, pagarbi, saugi, atitiktų teisinius reikalavimus ir būtų suderinta su organizacijos prekės ženklu.

1.3 Šios politikos tikslas – mažinti rizikas, susijusias su reputacijos žala, reglamentavimo reikalavimų pažeidimais, intelektinės nuosavybės praradimu ir nesankcionuotu atskleidimu viešai prieinamais kanalais.

1.4 Ši politika taip pat skatina atskaitomybę ir struktūruotą valdyseną visose skaitmeninės komunikacijos formose, kurios yra susijusios su organizacija arba daro jai poveikį.

2. Taikymo sritis

2.1 Ši politika taikoma visiems darbuotojams, rangovams, praktikantams ir trečiųjų šalių atstovams, kurie:

2.1.1 komunikuoja organizacijos vardu oficialiai arba neoficialiai;

2.1.2 viešojoje erdvėje nurodo arba suponuoja savo ryšį su organizacija;

2.1.3 naudoja asmenines ar organizacijos paskyras viešoms diskusijoms, susijusioms su organizacija.

2.2 Šios politikos taikomi komunikacijos kanalai apima, bet jais neapsiriboja:

2.2.1 socialinių tinklų platformas (pvz., LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook);

2.2.2 tinklaraščius, vikio sistemas, forumus ir viešas diskusijų lentas;

2.2.3 el. paštą arba tiesiogines žinutes išorės šalims (pvz., klientams, reguliuotojams, žiniasklaidai);

2.2.4 interviu spaudai, dalyvavimą diskusijų grupėse arba įrašytuose žiniasklaidos pasirodymuose;

2.2.5 dalyvavimą interneto bendruomenėse, kuriose minima organizacija.

2.3 Ši politika reglamentuoja tiek realiuoju laiku skelbiamą, tiek iš anksto suplanuotą turinį ir taikoma visiems įrenginiams bei paskyroms (asmeninėms ar organizacijos), naudojamiems komunikacijai skleisti.

3. Tikslai

3.1 Užkirsti kelią atsitiktiniam ar tyčiniam konfidencialios, jautrios ar reglamentuojamos informacijos atskleidimui per išorinės komunikacijos kanalus.

3.2 Užtikrinti, kad oficialūs vieši pareiškimai ir socialinių tinklų turinys būtų tikslūs, patvirtinti ir suderinti su organizacijos prekės ženklu, etika ir strategine komunikacija.

3.3 Užkirsti kelią reputacijos žalai ir užtikrinti nuoseklią komunikaciją tarp vidaus padalinių ir išorės platformų.

3.4 Laikytis taikomų teisinių pareigų, susijusių su viešais pareiškimais, įskaitant, bet tuo neapsiribojant, ES BDAR, NIS2 direktyvos, DORA reglamento ir sektoriui taikomų komunikacijos taisyklių reikalavimus.

3.5 Apibrėžti aiškias atsakomybes, leidžiamus naudojimo atvejus ir politikos taikymo protokolus visam personalui, vykdančiam viešai matomą veiklą.

4. Vaidmenys ir atsakomybės

4.1 Rinkodaros, komunikacijos arba viešųjų ryšių vadovas

4.1.1 Tvirtina visą oficialią organizacijos komunikaciją, skirtą viešam paskelbimui.

4.1.2 Prižiūri socialinių tinklų turinio kalendorius ir gaires, skirtas prekės ženklo nuoseklumui užtikrinti.

4.1.3 Stebi su organizacija susijusius paminėjimus internete ir matomumą žiniasklaidoje.

4.2 Informacijos saugumo vadovas (CISO) / saugumo komanda

4.2.1 Stebi skaitmenines platformas dėl duomenų nutekėjimo, apsimetinėjimo ar fišingo požymių.

4.2.2 Koordinuoja veiksmus su reagavimo į incidentus komandomis socialiniais tinklais grindžiamų atakų ar pažeidimų atveju.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Įgyvendinimas ir atitiktis

9.1 Ši politika yra privaloma visam į taikymo sritį patenkančiam personalui ir trečiosioms šalims. Nesilaikymas gali lemti:

9.1.1 oficialius įspėjimus;

9.1.2 laikiną arba nuolatinį prieigos prie platformų ar sistemų atšaukimą;

9.1.3 drausmines nuobaudas, įskaitant darbo ar sutartinių santykių nutraukimą;

9.1.4 teisminius procesus, jei išorinė komunikacija sukelia reputacijos žalą, duomenų saugumo pažeidimą arba neatitiktį reglamentavimo reikalavimams.

9.2 Drausminės priemonės

9.2.1 Vidaus pažeidimai (pvz., konfidencialių duomenų nutekinimas, organizacijos šmeižimas) lemia žmogiškųjų išteklių funkcijos įtraukimą, formalų tyrimą ir dokumentavimą darbuotojo byloje.

9.2.2 Kai taikoma, teisės funkcija imasi civilinių teisinių priemonių arba informuoja institucijas apie nusikalstamą veiką (pvz., apsimetinėjimą, nutekintą vidinę informaciją apie sandorius).

9.3 Atitikties stebėsena

9.3.1 Saugumo ir komunikacijos komandos turi vykdyti nuolatinę stebėseną dėl:

9.3.1.1 prekės ženklo paminėjimų pagrindinėse platformose;

9.3.1.2 neoficialaus organizacijos vaizdinės medžiagos ar prekių ženklų naudojimo;

9.3.1.3 žinomų rizikų (pvz., nepatenkintų darbuotojų, apsimetinėjimo bandymų).

9.3.2 Stebėsena turi atitikti darbuotojų privatumo teisės aktų ir reglamentų reikalavimus, o visi pažymėti atvejai turi būti patikrinti žmogaus.

9.4 Pranešėjų apsauga ir pranešimas apie netinkamą naudojimą

9.4.1 Kiekvienas darbuotojas, įtariantis šios politikos pažeidimą, skatinamas apie tai pranešti informacijos saugumo komandai, teisės funkcijai arba anonimiškai per pranešėjų portalą.

9.4.2 Bet kokios neigiamos pasekmės pranešėjui yra griežtai draudžiamos ir užtraukia nedelsiamas drausmines priemones.

10. Peržiūros ir atnaujinimo reikalavimai

10.1 Ši politika turi būti peržiūrima kasmet arba anksčiau, jeigu:

10.1.1 reikšmingai pasikeičia reglamentavimo reikalavimai (pvz., priimami nauji ES teisės aktai dėl skaitmeninės komunikacijos);

10.1.2 pradedamos naudoti naujos socialinių tinklų platformos arba komunikacijos kanalai;

10.1.3 įvyksta reikšmingas incidentas arba kartojasi pažeidimai, rodantys procesų spragas;

10.1.4 įvyksta struktūriniai ar vadovų pasikeitimai viešųjų ryšių, teisės ar saugumo funkcijose.

10.2 Peržiūrą turi bendrai atlikti:

10.2.1 rinkodaros / viešųjų ryšių vadovas;

10.2.2 CISO arba saugumo rizikos vadovas;

10.2.3 teisės ir atitikties pareigūnai.

10.3 Atnaujinimai turi būti dokumentuojami politikos pakeitimų registre ir komunikuojami per vidaus informuotumo kanalus. Kai atliekami esminiai pakeitimai, visi paveikti asmenys turi pakartotinai patvirtinti susipažinimą su politika.

11. Susijusios politikos ir sąsajos

11.1 Šią politiką palaiko ir su ja yra susiję šie organizacijos informacijos saugumo valdymo sistemos (ISVS) komponentai:

11.1.1 P1 – Informacijos saugumo politika: nustato bendruosius informacijos apsaugos principus, įskaitant reikalavimą užtikrinti, kad komunikacija nesukeltų nesankcionuoto atskleidimo.

11.1.2 P3 – Priimtino naudojimo politika: apibrėžia priimtiną elgseną skaitmeninėse platformose ir naudojantis technologijomis, tiesiogiai reglamentuodama asmeninį ir profesinį socialinių kanalų naudojimą.

11.1.3 P6 – Rizikos valdymo politika: nustato rizikos sistemą grėsmėms, susijusioms su viešąja komunikacija ir reputacine ekspozicija, vertinti.

11.1.4 P8 – Informacijos saugumo supratimo ugdymo ir mokymų politika: nustato informuotumo didinimo programų reikalavimus darbuotojams mokyti apie saugios komunikacijos praktiką ir socialinės inžinerijos grėsmes.

11.1.5 P13 – Duomenų klasifikavimo ir ženklinimo politika: nurodo personalui, kokia informacija laikoma ribojamo naudojimo ar konfidencialia ir negali būti atskleidžiama išorėje.

11.1.6 P30 – Reagavimo į incidentus politika: apibrėžia, kaip tvarkyti su viešąja komunikacija susijusius incidentus, įskaitant duomenų nutekėjimą, apsimetinėjimą ir reglamentavimo reikalavimų pažeidimus.

11.1.7 P33 – Audito ir atitikties stebėsenos politika: reglamentuoja audito procesus, kuriais patvirtinamos socialinių tinklų kontrolės priemonės, stebėsenos sistemos ir atitiktis išorinės komunikacijos politikoms.

12. Pamatiniai standartai ir sistemos

12.1 ISO/IEC 27001:

12.1.1 8.1 skyrius – veiklos planavimas ir kontrolė: reikalauja apibrėžtų procesų ir vaidmenimis grindžiamos valdysenos viešajai komunikacijai valdyti, užtikrinant tikslumą, tvirtinimo eigą ir su duomenų ar reputacijos rizika susijusių incidentų eskalavimą.

12.2 ISO/IEC 27002:2022:

12.2.1 Kontrolės priemonė 5.10 – informacijos naudojimas: reglamentuoja autorizuotą ir etišką vidaus bei išorinės komunikacijos sklaidą.

12.2.2 Kontrolės priemonė 5.11 – informacijos ir turto priimtinas naudojimas: stiprina priimtino naudojimo praktiką dalijantis turiniu naudojant organizacijos turtą arba asmenines paskyras.

12.2.3 Kontrolės priemonė 5.35 – ryšiai su institucijomis: reikalauja struktūruotos ir autorizuotos išorinės komunikacijos su reguliavimo institucijomis ir viešojo sektoriaus įstaigomis.

12.2.4 Kontrolės priemonė 5.36 – atitiktis politikoms ir standartams: užtikrina nuoseklų vidaus politikų taikymą visais komunikacijos atvejais.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – elgsenos taisyklės: reikalauja formalių sistemų ir komunikacijos naudojimo taisyklių, įskaitant viešo atskleidimo standartus.

12.3.2 AC-8 – pranešimas apie sistemos naudojimą: pagrindžia privalomų atsakomybės ribojimo pareiškimų ir turinio perspėjimų taikymą išorėje matomose platformose.

12.3.3 AU-12 – audito įrašų saugojimas: taikoma žurnalų ir komunikacijos istorijos išsaugojimui incidentų peržiūros ir audito tikslais.

12.4 ES BDAR (2016/679):

12.4.1 5 straipsnis – duomenų tvarkymo principai: draudžia nesankcionuotą asmens duomenų atskleidimą viešojoje komunikacijoje.

12.4.2 25 straipsnis – privatumas pagal projektavimą ir pagal numatytuosius nustatymus: reikalauja privatumo apsaugos priemonių komunikacijos priemonėse ir turinio tvirtinimo eigoje.

12.4.3 32 straipsnis – tvarkymo saugumas: taikoma šifravimui, prieigos kontrolei ir turinio tvirtinimo procesams.

12.4.4 33 straipsnis – pranešimas apie pažeidimą: nustato pareigą laiku pranešti apie asmens duomenų nutekėjimą per viešus kanalus.

12.5 ES NIS2 direktyva (2022/2555):

12.5.1 21 straipsnis – kibernetinio saugumo rizikos valdymo priemonės: apima komunikacijos protokolus ir pareigas incidentų metu bei viešojoje komunikacijoje apie riziką.

12.6 ES DORA reglamentas (2022/2554):

12.6.1 9 straipsnis – IRT rizikos valdymas: taikomas išoriškai inicijuojamoms komunikacijos rizikoms, tokioms kaip apsimetinėjimas, klaidinančios informacijos sklaida ir reputacijos trikdymas.

12.6.2 16 straipsnis – komunikacijos strategija: reikalauja, kad kritiniai finansų ar paslaugų teikėjai valdytų komunikacijos rizikas ir reagavimo veiksmus krizių scenarijuose.

12.7 COBIT 2019:

12.7.1 APO09 – valdomi paslaugų susitarimai ir komunikacija: reikalauja struktūruotos vidaus ir išorinės komunikacijos valdysenos.

12.7.2 DSS05 – saugumo paslaugų valdymas: užtikrina, kad komunikacijos veiklos nesukurtų papildomos rizikos ir nesusilpnintų incidentų valdymo procesų.