					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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	5.1, 5.2, 6.1, 8 skyriai	Vadovavimas, rizikos valdymas ir išorinės komunikacijos operacinės kontrolės
ISO/IEC 27002:2022	Kontrolės priemonės 5.10, 5.11	Priimtinas naudojimas ir informacijos saugumas komunikacijos metu
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Elgsenos taisyklės, auditas, pranešimas apie incidentus ir viešai prieinamo turinio bei prieigos valdymas
ES BDAR	5, 32, 33 straipsniai	Duomenų apsaugos principai, saugumas ir pranešimas apie pažeidimus, turinčius poveikį viešajai komunikacijai
ES NIS2 direktyva	21 straipsnio 2 dalies e ir f punktai	Politikos dėl sistemų naudojimo ir tiekimo grandinės bei viešosios komunikacijos rizikų valdymo
ES DORA reglamentas	14 straipsnio 4 dalis	Komunikavimo pareigos po incidentų

1. Tikslas

1.1. Ši politika nustato privalomus reikalavimus visai viešajai komunikacijai, įskaitant naudojimąsi socialiniais tinklais, bendravimą su žiniasklaida ir išorinį skaitmeninį turinį, kai minima įmonė, jos darbuotojai, klientai, sistemos ar vidinės praktikos.

1.2. Ši politika padeda apsaugoti įmonės reputaciją, užtikrinti atitiktį teisiniams ir reguliavimo reikalavimams bei sumažinti informacijos nutekėjimo, klaidinančios informacijos ar saugumo incidentų riziką.

1.3. Ji sudaro sąlygas darbuotojams ir partneriams pozityviai bei atsakingai dalyvauti internetinėse diskusijose, kartu išvengiant atsitiktinio informacijos atskleidimo ar klaidingo įmonės pozicijos pristatymo.

1.4. Ši politika stiprina MVĮ pasirengimą ISO/IEC 27001 sertifikavimui, nustatydama viešai arba išorės suinteresuotosioms šalims teikiamos informacijos kontrolę.

2. Taikymo sritis

2.1. Ši politika taikoma visiems su organizacija susijusiems asmenims, įskaitant:

2.1.1. darbuotojus ir rangovus;

2.1.2. laisvai samdomus specialistus, konsultantus ir trečiųjų šalių tiekėjus;

2.1.3. praktikantus ar ne visą darbo laiką dirbančius darbuotojus, dalyvaujančius teikiant paslaugas klientams arba turinčius prieigą prie sistemų.

2.2. Ši politika taikoma visoms išorinės komunikacijos formoms, kuriose minima organizacija, įskaitant:

2.2.1. įrašus socialiniuose tinkluose (LinkedIn, Twitter/X, TikTok, Instagram, Facebook ir kt.);

2.2.2. tinklaraščio įrašus, interneto forumus, klientų atsiliepimus ir diskusijų gijas;

2.2.3. viešus pasisakymus (pvz., konferencijose, internetiniuose seminaruose, tinklalaidėse);

2.2.4. el. laiškus ar žinutes žurnalistams, valdžios institucijų atstovams ar nuomonės formuotojams;

2.2.5. viešai bendrinamas ekrano kopijas, nuotraukas ar vaizdo įrašus iš darbo aplinkos.

2.3. Ši politika taip pat taikoma, kai tokia komunikacija vykdoma:

2.3.1. naudojant asmeninius įrenginius ar paskyras;

2.3.2. ne darbo metu;

2.3.3. nesant piktavališkų ketinimų — net atsitiktinės ar spontaniškos pastabos patenka į taikymo sritį, jei jose minima įmonė.

3. Tikslai

3.1. Reputacijos apsauga: užkirsti kelią žalai įmonės reputacijai dėl nesankcionuotos ar netinkamos viešosios komunikacijos.

3.2. Duomenų saugumas: išvengti netyčinio jautrių duomenų, vidinių sistemų ar klientų informacijos atskleidimo socialiniuose tinkluose ar viešuose kanaluose.

3.3. Teisinė ir reguliavimo atitiktis: užtikrinti, kad visas viešas turinys, kuriame minima įmonė, atitiktų taikomus duomenų apsaugos ir verslo komunikacijos teisės aktų reikalavimus.

3.4. Profesinis elgesys: skatinti atsakingą dalyvavimą internetinėse diskusijose ir bendravime su žiniasklaida, taip pat naudojant asmenines paskyras.

3.5. Pasirengimas incidentams: nustatyti aiškius ir praktiškai įgyvendinamus veiksmus atsitiktinio informacijos atskleidimo ar politikos pažeidimų atvejais.

4. Vaidmenys ir atsakomybės

4.1. Generalinis direktorius (GD)

4.1.1. yra šios politikos savininkas ir ją tvirtina;

4.1.2. peržiūri ir tvirtina visus viešus pareiškimus, komunikaciją su žiniasklaida ar interviu;

4.1.3. užtikrina, kad ši politika būtų aiškiai komunikuojama visiems darbuotojams ir trečiosioms šalims;

4.1.4. tiria šios politikos pažeidimus ir į juos reaguoja, derindamas veiksmus su reagavimo į incidentus procedūromis.

4.2. Paskirtas darbuotojas arba komunikacijos vadovas (jei paskirtas)

4.2.1. padeda GD, prieš išorinį paskelbimą peržiūrėdamas turinį (pvz., tinklaraščio įrašus, viešų pasisakymų temas);

4.2.2. tvarko patvirtintos žiniasklaidos veiklos ar didelės rizikos socialinių tinklų įrašų registrus;

4.2.3. pagal galimybes stebi viešai prieinamus įmonės paminėjimus internete dėl reputacijos ar saugumo rizikų.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Metinė peržiūra

9.1.1. Ši politika turi būti peržiūrima bent kartą per metus generalinio direktoriaus (GD).

9.1.2. Peržiūros metu turi būti užtikrinta atitiktis atnaujintiems teisiniams įpareigojimams, komunikacijos srities tendencijoms ir vidiniams verslo pokyčiams.

9.2. Peržiūra pagal suveikimo kriterijus

9.2.1. Ši politika turi būti nedelsiant atnaujinama po:

9.2.1.1. reikšmingo incidento socialiniuose tinkluose ar reputacijos problemos;

9.2.1.2. trečiųjų šalių tiekėjų, valdančių komunikaciją, pasikeitimo;

9.2.1.3. naujų teisės aktų ar reguliavimo įpareigojimų, susijusių su internetine komunikacija, žiniasklaida ar prekės ženklu.

9.3. Pakeitimų dokumentavimas

9.3.1. Visi atnaujinimai turi būti registruojami, nurodant peržiūros datą, pakeitimų santrauką ir GD patvirtinimą.

9.3.2. Audito ir sertifikavimo tikslais turi būti saugoma versijų istorija.

9.4. Atnaujinimų paskelbimas

9.4.1. Visi darbuotojai ir rangovai turi būti informuojami apie visus politikos pakeitimus.

9.4.2. Atnaujintos versijos turi būti platinamos el. paštu arba vidiniuose portaluose.

9.4.3. Bet kuris viešąją komunikaciją valdantis tiekėjas prieš tęsdamas veiklą turi patvirtinti atnaujintas sąlygas.

10. Susijusios politikos ir sąsajos

10.1. Ši politika taikoma kartu su šiomis MVĮ politikomis:

10.1.1. P3S – Priimtino naudojimo politika: nustato priimtiną elgesį naudojant komunikacijos platformas, įskaitant prieigą prie socialinių tinklų darbo metu.

10.1.2. P8S – Informacijos saugumo supratimo ir mokymo politika: užtikrina, kad darbuotojai būtų apmokyti atpažinti perteklinio informacijos atskleidimo, fišingo ar reputacinių grėsmių internete rizikas.

10.1.3. P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad asmens ir klientų duomenys nebūtų bendrinami išorinėje komunikacijoje, laikantis ES BDAR ir kitų teisinių reikalavimų.

10.1.4. P30S – Reagavimo į incidentus politika: reglamentuoja reagavimą į atsitiktinį viešą atskleidimą, internetines grėsmes ar reputacines atakas, kylančias dėl netinkamo socialinių tinklų naudojimo.

10.1.5. P37S – Teisinės ir reguliavimo atitikties politika: nustato platesnius organizacijos teisinius ir sutartinius įpareigojimus viešai dalijantis turiniu.

10.2. Šios politikos turi būti taikomos kartu, siekiant išlaikyti saugų, pagarbų ir teisės aktų reikalavimus atitinkantį organizacijos išorinį matomumą.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 5.1 punktas – Vadovavimas ir įsipareigojimas: reikalauja vadovybės priežiūros valdant reputacijos ir informacijos rizikas.

11.1.2. 6.1 punktas – rizikos valdymas: apima su komunikacija susijusias rizikos ekspozicijas.

11.1.3. 8.1 punktas – operacinė kontrolė: apima taisykles, kaip informacija perduodama išorėje.

11.2. ISO/IEC 27002

11.2.1. Kontrolė 5.10 – Priimtinas informacijos ir turto naudojimas.

11.2.2. Kontrolė 5.11 – Informacijos saugumas komunikacijoje.

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Elgsenos taisyklės: reglamentuoja tinkamą elgesį naudojant informacinius išteklius.

11.3.2. AU-7 – Audito duomenų mažinimas ir ataskaitų generavimas: palaiko viešo sistemų naudojimo stebėseną.

11.3.3. IR-6 – Pranešimas apie incidentus: nustato reagavimą į reputacijos ir komunikacijos pažeidimus.

11.3.4. AC-22 – Viešai prieinamas turinys: užtikrina išorinių publikacijų ir prieigos kontrolę.

11.4. ES BDAR (2016/679)

11.4.1. 5 straipsnis – Asmens duomenų tvarkymo principai (tikslumas, vientisumas, atskaitomybė).

11.4.2. 32 straipsnis – Tvarkymo saugumas: reikalauja apsaugos priemonių viešo dalijimosi atvejais.

11.4.3. 33 straipsnis – Pranešimas apie pažeidimą: taikomas, jei asmens duomenys atskleidžiami per išorinę komunikaciją.

11.5. ES NIS2 direktyva (2022/2555)

11.5.1. 21 straipsnio 2 dalies e punktas – politikos dėl informacinių sistemų naudojimo, įskaitant komunikacijos platformas.

11.5.2. 21 straipsnio 2 dalies f punktas – politikos dėl kibernetinio saugumo rizikų valdymo tiekimo grandinėje ir viešose platformose.

11.6. ES DORA reglamentas (2022/2554)

11.6.1. 14 straipsnio 4 dalis – komunikavimo pareigos klientams, trečiosioms šalims ir institucijoms po operacinių incidentų.

11.7. COBIT 2019

11.7.1. APO09 – Paslaugų susitarimų valdymas: apima tiekėjų ir su komunikacija susijusių trečiųjų šalių priežiūrą.

11.7.2. DSS05 – Saugumo paslaugų valdymas: apima viešai prieinamų skaitmeninių išteklių apsaugą.

11.7.3. EDM03 – Rizikos optimizavimo užtikrinimas: pabrėžia su komunikacija susijusių reputacijos ir atitikties rizikų valdymą.