					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P03S					Dokumento pavadinimas: **Priimtino naudojimo 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 taikomais standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	5 skyrius	Aktualu bendrai politikos taikymo sričiai ir įgyvendinimui
ISO/IEC 27002:2022	5.10, 5.11, 5	Pateikia gaires dėl priimtino naudojimo reikalavimų ir kontrolės priemonių
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Apima sistemų ir įrenginių naudojimą, stebėseną ir naudotojų mokymą
ES BDAR	5 straipsnio 1 dalies f punktas, 32 straipsnis	Duomenų vientisumas, konfidencialumas ir saugumo priemonės
ES NIS2 direktyva	21 straipsnio 2 dalies b punktas	Nustato reikalavimą taikyti tinkamas saugumo ir priimtino naudojimo politikas
ES DORA reglamentas	9 straipsnis	IRT rizikos valdymo politika, kontrolės priemonės ir jų taikymas
COBIT 2019	DSS05, BAI08	Saugumo paslaugos ir žinių valdymas

1. Tikslas

1.1. Ši politika nustato priimtiną, atsakingą ir saugų įmonės suteiktų sistemų, įrenginių, interneto prieigos, el. pašto, debesijos paslaugų ir bet kokių asmeninių įrenginių, naudojamų verslo tikslais, naudojimą.

1.2. Ji užtikrina, kad asmenys suprastų savo pareigas naudodamiesi organizacijos IT ištekliais ir saugodami duomenų vientisumą, privatumą bei veiklos tęstinumą.

1.3. Ši politika padeda užtikrinti atitiktį ISO/IEC 27001:2022, nustatydama aiškius naudotojų elgsenos standartus, suderintus su teisiniais, sutartiniais ir reguliavimo reikalavimais.

2. Taikymo sritis

2.1. Ši politika taikoma visiems asmenims, kurie gauna prieigą prie įmonės sistemų ar duomenų, juos valdo arba su jais sąveikauja, įskaitant:

2.1.1. darbuotojus ir rangovus;

2.1.2. laikinuosius darbuotojus ir praktikantus;

2.1.3. išorės IT paslaugų teikėjus.

2.2. Politika apima:

2.2.1. įmonei priklausančius kompiuterius, telefonus ir planšetes;

2.2.2. asmeninius įrenginius, patvirtintus naudoti verslo tikslais (BYOD);

2.2.3. įmonės tinklus, debesijos platformas ir programinės įrangos kaip paslaugos sprendimus;

2.2.4. interneto prieigą, el. pašto sistemas, bendras saugyklas ir verslo programas.

2.3. Ši politika taikoma visose darbo aplinkose – dirbant įmonės patalpose, nuotoliniu ar mišriuoju būdu – ir visą darbo laiką.

3. Tikslai

3.1. Apibrėžti, kas laikoma priimtinu ir nepriimtinu IT sistemų naudojimu.

3.1.1. Mažinti saugumo riziką, kylančią dėl netinkamo naudojimo, neteisėtos prieigos ar kenkėjiškos programinės įrangos įdiegimo.

3.1.2. Saugoti verslo duomenis, klientų informaciją ir įmonės reputaciją.

3.1.3. Nustatyti privalomas taisykles ir užtikrinti visų naudotojų atskaitomybę.

3.1.4. Užtikrinti stebėseną ir atitiktį, kad pažeidimai būtų nustatomi anksti ir būtų galima taikyti korekcinius veiksmus.

4. Vaidmenys ir atsakomybė

4.1. Generalinis direktorius

4.1.1. Tvirtina šią politiką ir užtikrina, kad jos taikymui būtų skirti reikiami ištekliai ir suteikti įgaliojimai.

4.1.2. Peržiūri ir tvirtina visas šios politikos išimtis.

4.2. IT vadovas arba išorės IT paslaugų teikėjas

4.2.1. Tvarko patvirtintos programinės ir techninės įrangos sąrašus.

4.2.2. Konfigūruoja įrenginius taip, kad būtų užtikrintas priimtino naudojimo taisyklių įgyvendinimas, pvz., turinio filtravimas ir prieigos žurnalų registravimas.

4.2.3. Stebi naudojimą dėl galimų pažeidimų ir tiria incidentus.

4.2.4. Užtikrina, kad asmeniniai įrenginiai (BYOD), naudojami verslo tikslais, būtų autorizuoti ir saugūs.

[... 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. IT vadovas privalo šią politiką peržiūrėti kasmet, o galutinį patvirtinimą turi suteikti generalinis direktorius, kad būtų užtikrinta jos atitiktis technologijų naudojimo praktikai, naujoms rizikoms ir atitikties prievolėms.

9.2. Tarpinės peržiūros priežastys

9.2.1. Peržiūros taip pat turi būti atliekamos reaguojant į:

9.2.2. naujas sistemas ar technologijas, pvz., naują debesijos paslaugą ar galinių įrenginių platformą;

9.2.3. reikšmingus politikos pažeidimus;

9.2.4. atnaujintus teisės aktus ar sutarties sąlygas, turinčias įtakos IT naudojimui.

9.3. Pakeitimų dokumentavimas

9.3.1. Visi atnaujinimai turi būti registruojami versijų žurnale, kuriame nurodoma:

9.3.1.1. versijos numeris;

9.3.1.2. peržiūros data;

9.3.1.3. pakeitimų santrauka;

9.3.1.4. tvirtinantis asmuo.

9.4. Politikos komunikavimas

9.4.1. Atnaujintos šios politikos versijos turi būti pateiktos visiems susijusiems naudotojams. Darbuotojai, vykdydami savo informuotumo apie saugumą pareigas, privalo patvirtinti jos gavimą ir supratimą.

10. Susijusios politikos ir sąsajos

10.1. Ši politika taikoma kartu su kitomis SME politikomis, siekiant užtikrinti visapusišką saugumo atsakomybių aprėptį:

10.1.1. P4S – Prieigos kontrolės politika: nustato techninį ir procedūrinį leidžiamo naudojimo bei paskyrų apribojimų taikymą.

10.1.2. P8S – Informacijos saugumo sąmoningumo didinimo ir mokymo politika: nustato naudotojų švietimą apie priimtino naudojimo ribas ir pranešimo pareigas.

10.1.3. P9S – Nuotolinio darbo politika: reglamentuoja įmonės sistemų naudojimą dirbant ne įmonės patalpose ar iš namų.

10.1.4. P17S – Duomenų apsaugos ir privatumo politika: nustato asmens duomenų tvarkymo taisykles, susijusias su priimtino naudojimo stebėsena ir BYOD.

10.1.5. P30S – Incidentų valdymo politika: nustato netinkamo naudojimo ar priimtino naudojimo sąlygų pažeidimų tyrimo ir reagavimo tvarką.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 5.10 punktas – reikalauja, kad organizacijos apibrėžtų ir užtikrintų priimtiną informacijos turto naudojimą.

11.2. ISO/IEC 27002

11.2.1. 5.10 kontrolės priemonė – pateikia gaires dėl priimtino sistemų naudojimo, įskaitant leidžiamą ir draudžiamą elgseną.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – apima sistemų naudojimo kontrolę, įskaitant asmeninius įrenginius.

11.3.2. AC-20 – reikalauja išorės sistemų autorizavimo ir stebėsenos.

11.3.3. AT-2 – pabrėžia naudotojų mokymą apie priimtino naudojimo praktiką.

11.4. ES BDAR

11.4.1. 5 straipsnio 1 dalies f punktas – reikalauja užtikrinti asmens duomenų vientisumą ir konfidencialumą, kurie gali būti pažeisti dėl netinkamo naudotojų elgesio.

11.4.2. 32 straipsnis – nustato pareigą įgyvendinti technines ir organizacines priemones sistemų ir duomenų saugumui užtikrinti.

11.5. ES NIS2 direktyva

11.5.1. 21 straipsnio 2 dalies b punktas – reikalauja taikyti tinkamas saugumo politikas, įskaitant priimtino naudojimo taisykles, siekiant mažinti kibernetines grėsmes.

11.6. ES DORA reglamentas

11.6.1. 9 straipsnis – reikalauja IRT rizikos valdymo politikų, apimančių naudojimo kontrolę ir taikymo mechanizmus.

11.7. COBIT 2019

11.7.1. DSS05 – Saugumo paslaugų valdymas: pabrėžia naudotojų elgsenos kontrolę pagal politikas.

11.7.2. BAI08 – Žinių valdymas: apima informuotumą apie politikos atsakomybes ir mokymą dėl priimtino naudojimo.