					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P12S					Dokumento pavadinimas: **Turto valdymo 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	8 punktas	Turto valdymo reikalavimai
ISO/IEC 27002:2022	5 kontrolė	Turto valdymo kontrolės priemonės
NIST SP 800-53 Rev.5	CM-8	Sistemų komponentų apskaita
ES NIS2 direktyva	21 straipsnio 2 dalies a punktas	Turto stebėsena tinklų ir informacinių sistemų apsaugai
ES DORA reglamentas	5 straipsnio 8 dalis	IRT turto apskaitos reikalavimai
COBIT 2019	BAI	IT turto gyvavimo ciklo valdymas
ES BDAR	30 straipsnis	Duomenų tvarkymo veiklų apskaita

1. Tikslas

1.1 Ši politika nustato, kaip organizacija identifikuoja, registruoja, apsaugo ir nurašo savo informacinį turtą, įskaitant fizinius ir skaitmeninius komponentus.

1.2 Šios politikos tikslas – mažinti veiklos ir saugumo riziką, užtikrinant viso veikloje naudojamo turto matomumą, atskaitomybę ir saugų tvarkymą viso jo gyvavimo ciklo metu.

1.3 Patikima turto apskaita padeda užtikrinti atitiktį reglamentavimo reikalavimams, reagavimą į incidentus, veiklos tęstinumo planavimą ir rizikos valdymą.

1.4 Ši politika taip pat padeda siekti ISO/IEC 27001 sertifikavimo ir parodo atitiktį teisiniams, finansiniams ir kibernetinio saugumo reikalavimams pagal tokius reikalavimų rinkinius kaip ES BDAR, NIS2 direktyva ir DORA reglamentas.

1.5 Mažoms ir vidutinėms įmonėms (MVĮ) paprastas, tačiau sistemingas turto valdymo metodas yra būtinas siekiant išvengti nevaldomų įrenginių, duomenų praradimo ar neigiamų audito rezultatų, ypač kai techniniai žmogiškieji ištekliai yra riboti.

2. Taikymo sritis

2.1 Ši politika taikoma visam organizacijos valdomam, nuomojamam ar kitu pagrindu naudojamam turtui, įskaitant turtą, naudojamą:

2.1.1 darbui biure

2.1.2 nuotolinio ar hibridinio darbo sąlygomis

2.1.3 lauko ar mobiliojo darbo veikloje

2.1.4 debesijos ir išorinių paslaugų aplinkose

2.2 Į šios politikos taikymo sritį įtraukiami, be kita ko, šie turto tipai:

2.2.1 aparatinė įranga: nešiojamieji kompiuteriai, stacionarieji kompiuteriai, monitoriai, telefonai, planšetės, USB laikmenos, maršrutizatoriai, spausdintuvai, atsarginių kopijų laikmenos

2.2.2 programinė įranga: įdiegtos taikomosios programos, SaaS paslaugos, operacinės sistemos, antivirusinė programinė įranga, licencijos

2.2.3 duomenų turtas: veiklos duomenų saugyklos, skaičiuoklės, klientų įrašai, programų pirminis kodas

2.2.4 skaitmeniniai identifikatoriai ir paslaugos: domenų vardai, skaitmeniniai sertifikatai, API raktai, el. pašto paskyros, prisijungimai prie debesijos paslaugų

2.2.5 prieigos priemonės: raktai, lustinės kortelės, prieigos pakabukai, biometriniai žetonai

2.3 Ši politika taikoma visiems darbuotojams, rangovams ir trečiųjų šalių paslaugų teikėjams, kurie tvarko organizacijos turtą.

2.4 Politika taip pat reglamentuoja trumpalaikį turtą (pvz., projektui skirtus nešiojamuosius kompiuterius), ilgalaikį turtą ir bendro naudojimo turtą, kuriuo naudojasi keli darbuotojai.

3. Tikslai

3.1 Sukurti ir nuolat palaikyti išsamią ir tikslią viso susijusio turto apskaitą, kuri būtų nuolat atnaujinama.

3.2 Užtikrinti, kad kiekvienam turto vienetui būtų priskirtas turto savininkas, atsakingas už jo naudojimą, apsaugą ir grąžinimą.

3.3 Klasifikuoti turtą pagal jautrumą, poveikį verslui arba reikšmingumą reglamentavimo reikalavimams, kad būtų galima taikyti skirtingus apsaugos lygius.

3.4 Nustatyti aiškias turto išdavimo, perpriskyrimo, priežiūros, pranešimo apie praradimą ir nurašymo procedūras.

3.5 Užtikrinti saugų turto tvarkymą viso jo gyvavimo ciklo metu ir tai, kad jame saugoma informacija būtų apsaugota arba saugiai sunaikinta turtą šalinant.

3.6 Sumažinti saugumo incidentų, kylančių dėl neapskaityto, negrąžinto ar netinkamai naudojamo organizacijos turto, tikimybę.

3.7 Padėti užtikrinti atitiktį taikomiems teisės aktams (pvz., ES BDAR atskaitomybės principui) ir kibernetinio saugumo sertifikavimo standartams.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius (GD)

4.1.1 Tvirtina šią politiką ir atsako už tai, kad turto valdymo praktika būtų įgyvendinta ir jos būtų laikomasi visoje organizacijoje.

4.1.2 Peržiūri ir tvirtina turto apskaitos atnaujinimus bei prireikus sankcionuoja turto nurašymą arba perdavimą.

4.1.3 Turi būti informuojamas apie bet kokį reikšmingą turto praradimą, vagystę ar netinkamą naudojimą.

4.2 IT vadovas arba paskirtasis turto administratorius

4.2.1 Tvarko turto apskaitą (pvz., skaičiuoklėje, užklausų valdymo sistemoje ar paprastoje turto stebėsenos priemonėje).

4.2.2 Priskiria turto savininkus ir seka būsenos pokyčius (pvz., naujas, naudojamas, remontuojamas, nurašytas).

4.2.3 Patikrina, kad visas išduotas turtas būtų dokumentuotas ir susietas su konkrečiu asmeniu arba organizaciniu padaliniu.

4.2.4 Užtikrina, kad klasifikavimo žymos būtų taikomos ir jų būtų laikomasi (pvz., Vidinis, Konfidencialus).

4.2.5 Koordinuoja turto susigrąžinimą, išvalymą ir išjungimą darbo santykių nutraukimo proceso metu arba turtą nurašant.

4.2.6 Apie neišspręstus turto neatitikimus praneša GD.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Ši politika turi būti peržiūrima bent kartą per metus ir kiekvieną kartą, kai:

9.1.1 įdiegiamos naujos technologijos arba atsiranda naujų turto tipų

9.1.2 pasikeičia turto stebėsenos procedūros (pvz., pradedamos naudoti naujos priemonės ar platformos)

9.1.3 nauji reglamentavimo reikalavimai daro poveikį turto atsekamumui arba sunaikinimui

9.1.4 incidentas arba auditas nustato dabartinės turto valdymo praktikos spragą

9.2 Peržiūrose turi dalyvauti GD ir IT vadovas; jos turi apimti turto tvarkymo procedūrų, apskaitos šablonų ir klasifikavimo gairių atnaujinimus.

9.3 Visi atnaujinimai turi būti dokumentuojami ir komunikuojami susijusiems darbuotojams. Turi būti saugomas pagal versijų kontrolę tvarkomas pakeitimų žurnalas.

10. Susijusios politikos ir sąsajos

10.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atskaitomybę už politikos valdymą ir IT operacijas.

10.2 P4S – Prieigos kontrolės politika: susieja turto naudojimą (pvz., nešiojamuosius kompiuterius, mobiliuosius įrenginius) su naudotojų prieigos teisėmis ir tapatybių valdymu.

10.3 P7S – Įdarbinimo ir darbo santykių nutraukimo politika: užtikrina, kad turto išdavimas ir susigrąžinimas būtų įtraukti į darbuotojų gyvavimo ciklo procesus.

10.4 P13S – Duomenų klasifikavimo ir ženklinimo politika: pateikia taisykles, pagal kurias nustatoma, ar turtas turi būti klasifikuojamas kaip Vidinis ar Konfidencialus.

10.5 P30S – Reagavimo į incidentus politika: nustato reagavimo procedūras, jei su turtu susijęs įvykis sukelia saugumo arba privatumo pažeidimą.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas: reikalauja taikyti operacines kontrolės priemones turtui valdyti ir jam apsaugoti viso naudojimo metu.

11.2 ISO/IEC 27002

11.2.1 5.9 kontrolė: nustato, kaip identifikuoti turtą, priskirti savininkus, jį klasifikuoti ir saugiai valdyti.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: reikalauja, kad organizacijos sudarytų ir palaikytų sistemų komponentų apskaitą, įskaitant aparatinę įrangą, programinę įrangą ir virtualų turtą.

11.4 ES BDAR

11.4.1 30 straipsnis: reikalauja dokumentuoti duomenų tvarkymo veiklas, o tam būtina žinoti, kur duomenys saugomi ir kokiame turte.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies a punktas: numato technines ir organizacines priemones, įskaitant turto stebėseną, skirtas tinklų ir informacinių sistemų apsaugai.

11.6 ES DORA reglamentas

11.6.1 5 straipsnio 8 dalis: finansų sektoriaus subjektai privalo palaikyti išsamią IRT turto apskaitą kaip IRT rizikos valdymo dalį.

11.7 COBIT 2019

11.7.1 BAI09: nustato, kad IT turtas turi būti valdomas viso jo gyvavimo ciklo metu – nuo įsigijimo iki nurašymo – aiškiai priskiriant savininkus ir taikant kontrolės priemones.