					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P12					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**

1. Tikslas

1.1 Ši politika nustato privalomus organizacinius reikalavimus, taikomus informacijos išteklių identifikavimui, klasifikavimui, valdymui ir apsaugai per visą jų gyvavimo ciklą. Ji užtikrina visos organizacijos mastu taikomą aparatinės įrangos, programinės įrangos, duomenų, debesijos ir nematerialiųjų informacijos išteklių valdyseną, įskaitant mobiliąsias, nuotolines ir trečiųjų šalių valdomas aplinkas.

1.2 Šios politikos tikslas – užtikrinti visišką organizacijos informacijos išteklių aplinkos matomumą, sudaryti sąlygas taikyti veiksmingas saugumo kontrolės priemones, priskirti savininkus, užtikrinti atitiktį ir atsakingai vykdyti eksploatacijos nutraukimą arba šalinimą.

1.3 Ši politika atitinka ISO/IEC 27001:2022 A priedo 5.9 kontrolės priemonę, nustatydama pareigą tvarkyti centralizuotą informacijos ir susijusio turto apskaitą. Ji užtikrina atskaitomybę, susiedama kiekvieną turto vienetą su turto savininku ir taikydama pagal verslo jautrumą bei reglamentavimo reikalavimus nustatytą klasifikacija grindžiamą apsaugą.

2. Taikymo sritis

2.1 Ši politika taikoma visiems darbuotojams, rangovams, trečiųjų šalių tiekėjams ir paslaugų teikėjams, kurie valdo, naudoja, pasiekia, saugo ar tvarko organizacijai priklausančius arba jos kontroliuojamus informacijos išteklius.

2.2 Taikymo sritis apima visas turto kategorijas, įskaitant:

2.2.1 Fizinį turtą: nešiojamuosius kompiuterius, stalinius kompiuterius, mobiliuosius įrenginius, keičiamąsias laikmenas, spausdintuvus, tinklo įrangą

2.2.2 Skaitmeninį turtą: programinę įrangą, taikomąsias programas, sistemų atvaizdus, duomenų bazes, atsarginių kopijų duomenis, šifravimo raktus

2.2.3 Informacijos išteklius: struktūrizuotus ir nestruktūrizuotus duomenis, ataskaitas, el. laiškus, intelektinę nuosavybę

2.2.4 Debesijos ir virtualųjį turtą: IaaS, SaaS, PaaS aplinkas, virtualiąsias mašinas, konteinerius

2.2.5 Loginį turtą: domenų vardus, licencijas, naudotojų paskyras, bazines konfigūracijas

2.3 Ši politika taip pat reglamentuoja turtą, naudojamą nuotolinio darbo, hibridinėse ar išorinėms paslaugoms perduotose aplinkose, užtikrindama apsaugą ir matomumą net tais atvejais, kai turtas fiziškai nėra organizacijos patalpose.

3. Tikslai

3.1 Tvarkyti išsamią, tikslią ir nuolat atnaujinamą visų organizacijos informacijos išteklių apskaitą, nurodant savininką, klasifikaciją ir vietą.

3.2 Priskirti turto savininkus, atsakingus už jų valdomo turto klasifikavimą, tvarkymą ir apsaugą pagal duomenų valdysenos ir saugumo politikas.

3.3 Taikyti tinkamą viso turto klasifikavimą ir ženklinimą, atsižvelgiant į jautrumą, kritiškumą ir reglamentavimo reikalavimus.

3.4 Apsaugoti turtą pagal jo klasifikaciją ir susijusią rizikos ekspoziciją, įskaitant saugojimą, prieigą, perdavimą ir šalinimą.

3.5 Užtikrinti turto grąžinimo ir saugaus sunaikinimo procedūrų taikymą darbo santykių nutraukimo proceso, sutarties nutraukimo ar turto gyvavimo ciklo pabaigos metu.

3.6 Užtikrinti atitiktį tokioms sistemoms ir reglamentams kaip ISO/IEC 27001, ES BDAR, NIS2 direktyva, DORA reglamentas ir COBIT 2019, taikant struktūruotą turto valdymą ir užtikrinant audituojamumą.

4. Vaidmenys ir atsakomybės

4.1 Vadovybė

4.1.1 Tvirtina Turto valdymo politiką ir užtikrina, kad jos visapusiškam įgyvendinimui būtų skirti reikiami ištekliai.

4.1.2 Yra galutinai atsakinga už tai, kad organizacijos turtas būtų apsaugotas ir valdomas laikantis reglamentavimo ir sutartinių įsipareigojimų.

4.2 Informacijos saugumo vadovas (CISO)

4.2.1 Yra Turto valdymo politikos savininkas ir užtikrina jos integraciją į platesnę organizacijos informacijos saugumo valdymo sistemą (ISVS).

4.2.2 Peržiūri šios politikos išimtis ir nukrypimus bei užtikrina rizika grindžiamų mažinimo priemonių taikymą.

4.2.3 Prižiūri periodinius auditus, susijusius su turto klasifikavimu, turto apskaitos vientisumu ir atitiktimi turto gyvavimo ciklo reikalavimams.

[... 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 ne rečiau kaip kartą per metus arba reaguojant į:

9.1.1 Teisinių ar reglamentavimo įsipareigojimų pokyčius, darančius įtaką turto klasifikavimo ar apskaitos reikalavimams

9.1.2 Naujų turto kategorijų ar valdymo platformų įdiegimą (pvz., debesijos aplinkoje veikiančias CMDB)

9.1.3 Audito išvadas arba saugumo incidentus, susijusius su netinkamu turto valdymu

9.1.4 Organizacinius pertvarkymus, darančius poveikį savininkystei ar gyvavimo ciklo kontrolės priemonėms

9.2 Peržiūros procesą inicijuoja IT turto valdytojas ir koordinuoja kartu su CISO, pirkimų, teisiniu padaliniu ir susijusių padalinių vadovais.

9.3 Tarpinės peržiūros taip pat gali būti inicijuojamos dėl:

9.3.1 Verslo padalinių įsigijimo arba atskyrimo

9.3.2 Tiekėjų pokyčių, darančių poveikį trečiųjų šalių valdomam turtui

9.3.3 Technologijų atnaujinimų, apimančių masinį eksploatacijos nutraukimą arba suteikimą

9.4 Visi šios politikos pakeitimai privalo:

9.4.1 Būti valdomi pagal versijų kontrolę ir saugomi ISVS saugykloje

9.4.2 Būti patvirtinti vadovybės

9.4.3 Apimti pakeitimų santrauką ir pagrindimą

9.4.4 Būti komunikuojami visoms susijusioms suinteresuotosioms šalims, prireikus atnaujinant procedūras arba sistemų mokymus

10. Susijusios politikos ir sąsajos

10.1 Ši politika taikoma kartu su toliau nurodytomis susijusiomis politikomis ir palaiko jų įgyvendinimą:

10.1.1 P4 – Prieigos kontrolės politika: užtikrina, kad turto matomumas būtų suderintas su prieigos teisėmis ir kontrolės mechanizmais sistemose bei duomenų aplinkose.

10.1.2 P7 – Įdarbinimo ir darbo santykių nutraukimo politika: reglamentuoja savalaikį fizinio ir loginio turto suteikimą bei grąžinimą darbuotojų kaitos metu.

10.1.3 P13 – Duomenų klasifikavimo ir ženklinimo politika: nustato privalomas turto klasifikavimo taisykles, kurios lemia ženklinimo, tvarkymo ir šalinimo procedūras.

10.1.4 P14 – Duomenų saugojimo ir šalinimo politika: apibrėžia saugaus skaitmeninio ir fizinio informaciją turinčio turto šalinimo terminus ir būdus.

10.1.5 P22 – Žurnalų tvarkymo ir stebėsenos politika: užtikrina turto prieigos ir naudojimo atsekamumą per sistemų žurnalavimą, galinių įrenginių matomumą ir elgsenos analizę.

10.1.6 P30 – Reagavimo į incidentus politika: palaiko greitą su turtu susijusių pažeidimų, tokių kaip prarasti nešiojamieji kompiuteriai ar neapskaitytos saugojimo laikmenos, lokalizavimą ir tyrimą.

10.2 Šios politikos sudaro vientisą valdysenos struktūrą, užtikrinančią, kad turtas būtų saugiai valdomas, tiksliai apskaitomas ir tinkamai tvarkomas per visą jo gyvavimo ciklą.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintais informacijos saugumo standartais ir reglamentavimo sistemomis, pagal kurias reikalaujama užtikrinti patikimą turto valdymą per visą gyvavimo ciklą.

11.2 ISO/IEC 27001:

11.2.1 8 skyrius – reikalauja, kad organizacijos planuotų, įgyvendintų ir kontroliuotų procesus, reikalingus informacijos saugumo reikalavimams įvykdyti, įskaitant turto gyvavimo ciklo valdymo procesus.

11.3 ISO/IEC 27002:2022 – kontrolės priemonės 5.9–5.11

11.3.1 5.9 kontrolės priemonė – informacijos ir kito susijusio turto apskaita: reikalauja aktualios ir išsamios viso su informacijos tvarkymu susijusio turto apskaitos.

11.3.2 5.10 kontrolės priemonė – informacijos ir turto priimtinas naudojimas: palaikoma naudojimo taisyklėmis, savininkyste ir grąžinimo procesais.

11.3.3 5.11 kontrolės priemonė – turto grąžinimas: įgyvendinama taikant formalias perdavimo ir eksploatacijos nutraukimo procedūras.

11.3.4 Šios kontrolės priemonės nustato struktūruotus organizacijos turto identifikavimo, ženklinimo, priežiūros ir stebėsenos reikalavimus, taip pat atitinkamas savininkų ir patikėtinių atsakomybes per visą gyvavimo ciklą.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 – sistemos komponentų apskaita: įgyvendinama taikant centralizuotą turto valdymą, matomumą realiuoju laiku ir sąsajas su eksploatacinėmis konfigūracijomis.

11.4.2 RA-3 – rizikos vertinimas: turto apskaita yra pagrindinis elementas grėsmių modeliavimui ir rizikos vertinimui.

11.4.3 MP-6 – laikmenų išvalymas: užtikrinama taikant saugaus šalinimo metodus, apibrėžtus turto gyvavimo ciklo kontrolės priemonėse ir duomenų šalinimo politikoje.

11.5 ES BDAR (2016/679):

11.5.1 30 straipsnis – tvarkymo veiklos įrašai: reikalauja, kad organizacijos dokumentuotų sistemas, įrenginius ir saugyklas, kuriose saugomi arba tvarkomi asmens duomenys.

11.5.2 32 straipsnis – tvarkymo saugumas: atitinka turto pagrindu atliekamą rizikos vertinimą ir apsaugos priemones, pritaikytas klasifikuotam turtui ir kritinei infrastruktūrai.

11.6 ES NIS2 direktyva (2022/2555):

11.6.1 21(2)(a, b) straipsniai: nustato turto matomumą ir apskaitą kaip pagrindą rizikos analizei, apsaugai ir reagavimui į kibernetinio saugumo incidentus.

11.6.2 21(3) straipsnis: pabrėžia struktūruotos turto valdysenos būtinybę kaip organizacijos saugumo kultūros dalį.

11.7 ES DORA reglamentas (2022/2554):

11.7.1 5 straipsnis – IRT valdysena ir vidaus kontrolė: reikalauja, kad finansų subjektai valdytų IRT turtą, taikydami aiškius apskaitos, savininkystės ir apsaugos reikalavimus.

11.7.2 9 straipsnis – IRT rizikos valdymo sistema: nustato, kad turto valdymo procesai turi palaikyti grėsmių mažinimą, veiklos tęstinumo planavimą ir paslaugų atsparumą.

11.8 COBIT 2019:

11.8.1 BAI09 – turto valdymas: tiesiogiai atitinka struktūruotą organizacijos turto identifikavimą, klasifikavimą, naudojimą ir šalinimą.

11.8.2 DSS01 – valdomos operacijos: palaiko kontrolės priemonių, užtikrinančių turto apsaugą ir nuolatinę eksploatacinę valdyseną, įgyvendinimą.

11.8.3 MEA03 – atitikties stebėsena, vertinimas ir analizė: užtikrina reguliarų turto valdymo kontrolės priemonių auditą ir jų veiksmingumo vertinimą atitikties reglamentavimo reikalavimams požiūriu.