					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P04S					Dokumento pavadinimas: **Prieigos kontrolės 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 taikytinais standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	5 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1–AC-5	
ES BDAR	32 straipsnis	
ES NIS2 direktyva	21 straipsnio 2 dalies b punktas	
ES DORA reglamentas	9 straipsnis	
COBIT 2019	APO07, DSS01	

1. Tikslas

1.1. Ši politika nustato, kaip organizacija valdo prieigą prie sistemų, duomenų ir patalpų, kad informaciją pagal veiklos poreikį galėtų pasiekti tik įgalioti asmenys.

1.2. Joje nustatomos aiškios naudotojų prieigos suteikimo, keitimo, stebėsenos ir panaikinimo taisyklės, siekiant sumažinti neleistinos prieigos riziką ir užtikrinti atitiktį taikytiniems teisės aktams bei standartams.

1.3. Ši politika įtvirtina mažiausių būtinų teisių principą, pagal kurį prieiga turi būti apribota iki minimumo, būtino darbo funkcijoms atlikti.

2. Taikymo sritis

2.1. Ši politika taikoma visiems asmenims, kurie naudoja organizacijos IT sistemas, tinklus, duomenis ar patalpas arba valdo prieigą prie jų, įskaitant:

2.1.1. darbuotojus

2.1.2. rangovus

2.1.3. laikinuosius darbuotojus

2.1.4. išorės IT paslaugų teikėjus

2.2. Politika apima prieigą prie:

2.2.1. įmonės taikomųjų programų, bendrinamų failų išteklių ir duomenų bazių

2.2.2. el. pašto, VPN ir nuotolinės prieigos sistemų

2.2.3. veiklos tikslais naudojamų debesijos paslaugų

2.2.4. fizinės prieigos prie saugomų patalpų, pavyzdžiui, biurų ar serverinių

2.3. Ši politika yra privaloma visiems įrenginiams (įmonės suteiktiems ar patvirtintiems BYOD), platformoms ir vietoms.

3. Tikslai

3.1. Užtikrinti, kad prieigos teisės būtų suteikiamos tik gavus formalų patvirtinimą pagal pareigas ir veiklos pagrindimą.

3.2. Užkirsti kelią neleistinai ar perteklinei prieigai prie jautrių duomenų, sistemų ar infrastruktūros.

3.3. Nustatyti aiškias naudotojų prieigos suteikimo, keitimo ir panaikinimo procedūras.

3.4. Nustatyti privalomas reguliarias prieigos peržiūras ir automatizuotą arba rankinį žurnalų tvarkymą, kad būtų užtikrintas pasirengimas auditui.

3.5. Užtikrinti techninį prieigos apribojimų įgyvendinimą pasitelkiant konfigūravimą ir stebėseną.

4. Vaidmenys ir atsakomybės

4.1. Generalinis direktorius

4.1.1. Tvirtina šią politiką ir užtikrina, kad būtų skirti ištekliai veiksmingoms prieigos kontrolės priemonėms įgyvendinti.

4.1.2. Tvirtina išimtis ir peržiūri metinių prieigos auditų rezultatus.

4.2. IT vadovas / išorės IT paslaugų teikėjas

4.2.1. Vykdo naudotojų paskyrų sukūrimą, keitimą ir panaikinimą.

4.2.2. Tvarko prieigos kontrolės registrą, kuriame fiksuojama visa veikla (sukūrimas, keitimas, panaikinimas).

4.2.3. Įgyvendina vaidmenimis grindžiamą prieigos kontrolę (RBAC) ir taiko stiprų autentifikavimą (pvz., MFA).

4.2.4. Peržiūri prieigos žurnalus, siekdamas nustatyti įtartiną veiklą, ir apie nustatytas problemas informuoja generalinį direktorių.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Metinė politikos peržiūra

9.1.1. IT vadovas privalo peržiūrėti šią politiką kasmet. Bet kokie teisinio, techninio ar organizacinio konteksto pokyčiai turi lemti nedelsiamą jos atnaujinimą.

9.2. Peržiūros priežastys

9.2.1. Politika taip pat turi būti peržiūrima, jei įvyksta bent viena iš šių aplinkybių:

9.2.2. esminiai sistemų pakeitimai arba migravimas į debesijos aplinką

9.2.3. vaidmenų arba organizacinės struktūros pokyčiai

9.2.4. saugumo incidentas, susijęs su neleistina prieiga

9.2.5. reguliaciniai pokyčiai (pvz., ES BDAR, NIS2 direktyvos ar DORA reglamento atnaujinimai)

9.3. Pakeitimų dokumentavimas ir komunikavimas

9.3.1. Pakeitimai turi būti registruojami versijų istorijoje, tvirtinami generalinio direktoriaus ir komunikuojami visiems susijusiems darbuotojams.

9.4. Prieinamumas ir mokymai

9.4.1. Ši politika turi būti prieinama visiems darbuotojams, o susiję mokymai turi būti rengiami įdarbinimo metu ir vėliau ne rečiau kaip kartą per metus.

10. Susijusios politikos ir sąsajos

10.1. Ši politika turi būti taikoma kartu su šiomis MVĮ politikomis, siekiant visapusiškai užtikrinti saugios prieigos praktikos taikymą:

10.1.1. P3S – Priimtino naudojimo politika: užtikrina, kad naudotojai suprastų priimtiną elgesį naudojantis suteikta prieiga.

10.1.2. P5S – Pakeitimų valdymo politika: užtikrina, kad prieigos teisės atitiktų patvirtintus sistemų pakeitimus.

10.1.3. P7S – Įdarbinimo ir darbo santykių nutraukimo politika: nustato naudotojų prieigos suteikimo ir panaikinimo inicijavimo momentus.

10.1.4. P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad prieigos kontrolės priemonės atitiktų asmens duomenų apsaugos reikalavimus.

10.1.5. P30S – Reagavimo į incidentus politika: nustato, kaip valdomi ir tiriami su prieiga susiję incidentai (pvz., netinkamas naudojimas ar pažeidimai).

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 5.15 punktas – reikalauja formalizuotų prieigos kontrolės politikų ir procesų.

11.2. ISO/IEC 27002

11.2.1. 5.15–5.17 kontrolės priemonės – pateikia išsamias gaires dėl vaidmenimis grindžiamos prieigos kontrolės, naudotojų gyvavimo ciklo valdymo ir privilegijuotos prieigos valdymo.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1–AC-5 – reikalauja struktūrizuotų prieigos valdymo politikų, įskaitant paskyrų autorizavimą, peržiūrą ir stebėseną.

11.4. ES BDAR

11.4.1. 32 straipsnis – reikalauja techninių ir organizacinių kontrolės priemonių (pvz., prieigos valdymo), siekiant užtikrinti duomenų saugumą ir konfidencialumą.

11.5. ES NIS2 direktyva

11.5.1. 21 straipsnio 2 dalies b punktas – nustato privalomas operacines prieigos kontrolės ir tapatybių valdymo priemones, skirtas užkirsti kelią neleistinai prieigai prie sistemų.

11.6. ES DORA reglamentas

11.6.1. 9 straipsnis – pabrėžia saugų IRT rizikos valdymą, įskaitant patikimą prieigos kontrolę finansų sektoriaus subjektams.

11.7. COBIT 2019

11.7.1. APO07 – valdomas saugumas: numato apibrėžtas ir taikomas atsakomybes už prieigos valdymą.

11.7.2. DSS01 – operacijų valdymas: apima loginės prieigos valdymo procedūras ir saugios operacinės aplinkos palaikymą.