					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P04					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 taikomais standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	5.15, 5.17, 5 skyriai	Loginės ir fizinės prieigos valdymas
ISO/IEC 27002:2022	8.2, 8 kontrolės priemonės	Vaidmenimis grindžiama prieiga ir tapatybių valdymas
NIST SP 800-53 Rev.5	AC-1–AC-20, IA-1–IA-8	Paskyrų ir prieigos kontrolės priemonės, tapatybės nustatymas ir autentifikavimas
ES BDAR	5 straipsnio 1 dalies f punktas, 32 straipsnio 1 dalies b punktas; 39 konstatuojamoji dalis	Duomenų apsauga ir minimizavimas
ES NIS2 direktyva	21 straipsnio 2 dalies c–e punktai	Prieigos kontrolė, naudotojų autentifikavimas ir turto apsauga
ES DORA reglamentas	6 straipsnis, 9 straipsnio 2 dalis	IRT ir naudotojų prieiga bei griežtos kontrolės priemonės / trečiosios šalys
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA	Įdarbinimo pradžia, operacijos, stebėsena, atitiktis

1. Tikslas

1.1 Ši politika nustato privalomus principus, atsakomybes ir kontrolės reikalavimus, taikomus prieigai prie informacinių sistemų, taikomųjų programų, fizinių patalpų ir duomenų turto visoje organizacijoje valdyti.

1.2 Ji užtikrina, kad prieiga būtų suteikiama pagal verslo poreikį, pareigines funkcijas ir rizikos lygį, taikant mažiausių teisių, būtinybės žinoti ir pareigų atskyrimo principus.

1.3 Ši politika padeda įgyvendinti ISO/IEC 27001:2022 5.15 skyrių ir susijusias kontrolės priemones, reglamentuojančias loginę ir fizinę prieigą, naudotojų autentifikavimą ir prieigos gyvavimo ciklo valdymą.

1.4 Ši politika užtikrina skaitmeninių ir fizinių išteklių apsaugą nuo neleistino naudojimo, piktnaudžiavimo ar kompromitavimo.

2. Taikymo sritis

2.1 Ši politika taikoma visiems naudotojams, sistemoms ir patalpoms, patenkančioms į ISVS taikymo sritį, įskaitant:

2.1.1 darbuotojus, rangovus, tiekėjus ir laikinąjį personalą;

2.1.2 vietinę infrastruktūrą, debesijos sistemas ir hibridines aplinkas;

2.1.3 visą organizacijos turtą – aparatinę įrangą, programinę įrangą, duomenis ir saugias fizines zonas;

2.1.4 loginę prieigą (pvz., prie sistemų, tinklų, taikomųjų programų, API) ir fizinę prieigą (pvz., prie pastatų, duomenų centrų).

2.2 Ji reglamentuoja prieigą per visą tapatybės ir sąveikos su ištekliais gyvavimo ciklą – nuo įdarbinimo pradžios ir prieigos suteikimo iki pareigų pasikeitimo ir darbo ar sutartinių santykių pabaigos.

2.3 Politika taip pat apima asmeninių įrenginių naudojimo darbui (BYOD) ir nuotolinės prieigos atvejus, užtikrinant, kad kontrolės priemonės būtų nuosekliai taikomos nepriklausomai nuo vietos ir įrenginio nuosavybės modelio.

3. Tikslai

3.1 Įgyvendinti saugias, vaidmenimis grindžiamas prieigos kontrolės priemones, kurios palaiko veiklos vientisumą ir atitiktį reglamentavimo reikalavimams.

3.2 Užtikrinti, kad prieigos teisės būtų tinkamai tvirtinamos, stebimos ir laiku panaikinamos.

3.3 Užkirsti kelią neleistinai prieigai, teisių išplėtimui ar pasenusių prieigos teisių išlikimui.

3.4 Remti nulinio pasitikėjimo principus, numatant, kad prieiga draudžiama, jei ji nėra aiškiai patvirtinta ir pagrįsta.

3.5 Suteikti auditoriams ir suinteresuotosioms šalims užtikrintumą, taikant dokumentuotais įrodymais grindžiamas automatizuotas prieigos peržiūras ir politikos vykdymą.

3.6 Integruoti prieigos kontrolę į verslo procesus, personalo gyvavimo ciklo įvykius ir techninę architektūrą.

4. Vaidmenys ir atsakomybės

4.1 Vykdomoji vadovybė

4.1.1 Tvirtina prieigos kontrolės politiką ir užtikrina tinkamą biudžetą bei žmogiškuosius išteklius jai įgyvendinti.

4.1.2 Vadovybės peržiūrų metu vertina prieigos kontrolės rizikas ir strateginiu lygmeniu paskirsto atskaitomybę.

4.2 CISO / ISVS vadovas

4.2.1 Atsako už prieigos kontrolės sistemą ir užtikrina jos atitiktį ISO/IEC 27001 ir susijusiems standartams.

4.2.2 Koordinuoja politikos taikymą, kontrolės priemonių testavimą ir prieigos kontrolės rodiklių teikimą.

4.2.3 Prižiūri rizika grindžiamą prieigos modeliavimą ir stebi sistemines kontrolės spragas.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Peržiūros priežastys ir dažnumas

9.1.1 Ši politika turi būti peržiūrima:

9.1.1.1 kasmet; arba

9.1.1.2 po reikšmingo IT infrastruktūros, reglamentavimo reikalavimų ar rizikos lygio pokyčio;

9.1.1.3 po incidentų, kurie atskleidžia prieigos kontrolės silpnybes;

9.1.1.4 kai įvyksta reikšmingi autentifikavimo technologijų ar tapatybių platformų pokyčiai.

9.2 Peržiūros atsakomybė ir procesas

9.2.1 CISO arba paskirtas ISVS vadovas valdo peržiūros ciklą, įtraukdamas:

9.2.1.1 vidaus audito išvadas;

9.2.1.2 prieigos peržiūrų rezultatus ir rodiklius;

9.2.1.3 teisės ir reglamentavimo atnaujinimus;

9.2.1.4 technologinių platformų pokyčius.

9.2.2 Visi pakeitimai turi būti patvirtinti vykdomosios vadovybės ir komunikuoti visoms suinteresuotosioms šalims.

9.2.3 Esant reikšmingiems atnaujinimams, paveikti naudotojai gali būti įpareigoti iš naujo patvirtinti susipažinimą su politika.

9.3 Versijų kontrolė ir dokumentavimas

9.3.1 Pagrindinė versija turi būti saugoma ISVS dokumentų saugykloje kartu su šiais metaduomenimis:

9.3.1.1 versijos numeriu ir pakeitimų žurnalu;

9.3.1.2 įsigaliojimo data ir kitos peržiūros data;

9.3.1.3 savininku ir tvirtinančiu asmeniu;

9.3.1.4 platinimo ir susipažinimo patvirtinimo įrašais.

9.3.2 Pakeistos versijos turi būti archyvuojamos ir prieinamos ne trumpiau kaip 3 metus.

10. Susijusios politikos ir sąsajos

10.1 Ši politika funkciškai priklauso nuo toliau nurodytų politikų ir turi būti aiškinama kartu su jomis:

10.1.1 P01 – Informacijos saugumo politika: apibrėžia organizacijos įsipareigojimą saugumui ir aukšto lygio prieigos kontrolės lūkesčius.

10.1.2 P03 – Priimtino naudojimo politika: nustato elgsenos sąlygas prieigai ir naudotojų atskaitomybę už atsakingą sistemų naudojimą.

10.1.3 P05 – Pakeitimų valdymo politika: reglamentuoja, kaip prieigos konfigūracijų, vaidmenų ar grupių struktūrų pakeitimai turi būti saugiai įgyvendinami ir testuojami.

10.1.4 P07 – Įdarbinimo pradžios ir nutraukimo politika: nustato prieigos teisių suteikimą ir panaikinimą pagal naudotojo gyvavimo ciklo įvykius.

10.1.5 P11 – Naudotojų paskyrų ir privilegijų valdymo politika: detalizuoja paskyrų lygmens kontrolės priemones ir papildo šią politiką techninėmis prieigos kontrolės įgyvendinimo gairėmis.

10.2 Kartu šios politikos sudaro nuoseklią ir vykdytiną prieigos valdysenos sistemą visiems verslo padaliniams ir technologijoms.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:2022

11.1.1 5.15 skyrius – Prieigos kontrolė: ši politika įgyvendina reikalavimą kontroliuoti prieigą prie informacijos ir kito susijusio turto pagal verslo ir informacijos saugumo reikalavimus.

11.1.2 5.17 skyrius – Tapatybių valdymas ir 5.18 skyrius – Autentifikavimo informacija: šie reikalavimai įgyvendinami per tapatybių suteikimą, autentifikavimo mechanizmus ir privilegijų priskyrimą.

11.1.3 A priedo 8.2 (Prieigos kontrolės politika) ir 8.3 (Tapatybių valdymas) kontrolės priemonės: sudaro šios politikos kontrolės tikslų pagrindą, įskaitant vaidmenimis grindžiamą prieigą, naudotojo gyvavimo ciklo integraciją ir privilegijuotosios prieigos apsaugą.

11.2 NIST SP 800-53 Rev.

11.2.1 AC šeima (AC-1–AC-20): ši politika palaiko NIST prieigos kontrolės reikalavimus tiek fizinėms, tiek loginėms sistemoms, įskaitant politikos apibrėžimą (AC-1), paskyrų valdymą (AC-2) ir pareigų atskyrimą (AC-5).

11.2.2 IA šeima (IA-1–IA-8): pateikia gaires dėl tapatybės autentifikavimo, prisijungimo duomenų apsaugos ir MFA.

11.2.3 AU-2, AU-12: pagal šią politiką taikomi žurnalavimo ir audito reikalavimai palaiko naudotojų atskaitomybę ir incidentų tyrimą.

11.2.4 PE-2–PE-6: apima fizinės prieigos apribojimus, kuriuos ši politika iš dalies įgyvendina per leidimų korteles ir pastatų prieigos leidimus.

11.3 ES BDAR (2016/679)

11.3.1 5 straipsnio 1 dalies f punktas: asmens duomenys turi būti apsaugoti nuo neleistinos prieigos. Ši politika užtikrina techninį ir procedūrinį šio principo taikymą.

11.3.2 32 straipsnio 1 dalies b punktas: reikalauja įgyvendinti prieigos kontrolės priemones, pseudonimizavimą ir šifravimą, kad būtų užkirstas kelias neleistinam asmens duomenų tvarkymui.

11.3.3 39 konstatuojamoji dalis: reikalauja minimizuoti prieigą prie asmens duomenų, o šioje politikoje tai užtikrinama mažiausių teisių ir prieigos pagrindimo reikalavimais.

11.4 ES NIS2 direktyva (2022/2555)

11.4.1 21 straipsnio 2 dalies c–e punktai: ši politika leidžia taikyti technines ir organizacines prieigos kontrolės, naudotojų autentifikavimo ir turto apsaugos priemones esminiams ir svarbiems subjektams.

11.5 ES DORA reglamentas (2022/2554)

11.5.1 6 straipsnis: reikalauja IRT rizikos valdymo politikų, kurios aiškiai apimtų naudotojų prieigos valdymą ir tapatybės gyvavimo ciklo kontrolės priemones. Ši politika atitinka šį reikalavimą finansų ir IRT paslaugų sektoriuose.

11.5.2 9 straipsnio 2 dalis: ši politika palaiko griežtų prieigos kontrolės priemonių taikymą kaip trečiųjų šalių ir grupės vidaus IRT paslaugų valdymo dalį.

11.6 COBIT 2019

11.6.1 APO07 – Personalo išteklių valdymas: įgyvendina įdarbinimo pradžios ir užbaigimo kontrolės priemones prieigos valdysenai palaikyti.

11.6.2 BAI03 – Sprendimų identifikavimo ir kūrimo valdymas: integruoja prieigos kontrolės reikalavimus į sistemų projektavimą ir pakeitimų procesus.

11.6.3 DSS01 – Operacijų valdymas ir DSS05 – Saugumo paslaugų valdymas: reglamentuoja loginės prieigos apribojimų taikymą ir pažeidimų stebėseną.

11.6.4 MEA03 – Atitikties stebėsena, vertinimas ir įvertinimas: palaiko audito ir užtikrinimo mechanizmus, skirtus prieigos kontrolės veiksmingumui patvirtinti.