					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P11					Dokumento pavadinimas: **Naudotojų paskyrų ir privilegijų 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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	6.1.3 skyrius, 8 skyrius	-
ISO/IEC 27002:2022	Kontrolės priemonės 5.15–5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2–IA-5, AU-2, AU-12	-
ES BDAR	5 straipsnio 1 dalies f punktas, 32 straipsnis, 39 konstatuojamoji dalis	-
ES NIS2 direktyva	21 straipsnio 2 dalies a, d punktai, 21 straipsnio 3 dalis	-
ES DORA reglamentas	5, 9 straipsniai	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Tikslas

1 Ši politika nustato privalomas naudotojų paskyrų ir privilegijų valdymo kontrolės priemones visose informacinėse sistemose ir paslaugose. Ji užtikrina, kad prieiga prie organizacijos išteklių būtų suteikiama remiantis patikrinta tapatybe, vaidmens būtinybe, mažiausių privilegijų ir pareigų atskyrimo principais.

1.1 Ji padeda įgyvendinti organizacijos įsipareigojimą užtikrinti informacijos saugumą, taikant struktūrizuotus ir audituojamus paskyrų suteikimo, privilegijų priskyrimo, naudojimo stebėsenos ir paskyrų panaikinimo procesus.

1.2 Ši politika yra svarbi mažinant neteisėtos prieigos, netinkamo privilegijų naudojimo, vidinių grėsmių ir neatitikties taikomiems teisės aktų bei reglamentavimo reikalavimams riziką.

2. Taikymo sritis

2.1 Ši politika taikoma visiems darbuotojams, rangovams, trečiųjų šalių paslaugų teikėjams, konsultantams ir kitiems asmenims, kuriems suteikta prieiga prie organizacijos IT išteklių, taikomųjų programų ar duomenų.

2.2 Ji reglamentuoja visas sistemas ir aplinkas, kuriose taikomi naudotojų autentifikavimo ir prieigos kontrolės mechanizmai, įskaitant, bet neapsiribojant:

2.2.1 Įmonės taikomosiomis programomis ir duomenų bazėmis

2.2.2 Debesijos platformomis ir SaaS aplinkomis

2.2.3 Operacinėmis sistemomis ir administravimo konsolėmis

2.2.4 Nuotolinės prieigos priemonėmis ir VPN

2.2.5 Tapatybės ir prieigos valdymo (IAM) sistemomis

2.3 Politika apima tiek standartines, tiek privilegijuotas naudotojų paskyras ir nustato kontrolės priemones, susijusias su:

2.3.1 Paskyrų kūrimu, keitimu ir išjungimu

2.3.2 Privilegijų suteikimu ir delegavimu

2.3.3 Sesijų kontrole ir stebėsena

2.3.4 Autentifikavimo metodais ir prisijungimo duomenų valdymu

3. Tikslai

3.1 Užtikrinti, kad visos naudotojų paskyros būtų unikaliai identifikuotos, tinkamai autorizuotos ir priskiriamos tik po formalaus poreikio patvirtinimo.

3.2 Įgyvendinti mažiausių privilegijų principą ir užkirsti kelią nereikalingai ar perteklinei prieigai, taikant griežtas privilegijuotų paskyrų suteikimo ir naudojimo kontrolės priemones.

3.3 Užtikrinti, kad paskyrų būsena būtų laiku atnaujinama atsižvelgiant į darbo santykių ar vaidmens pokyčius, įskaitant nedelsiamą išjungimą darbo santykiams pasibaigus.

3.4 Sudaryti sąlygas proaktyviai nustatyti ir šalinti neaktyvias, netinkamai naudojamas ar neautorizuotas paskyras, pasitelkiant žurnalus, peržiūras ir automatizavimą.

3.5 Užtikrinti atitiktį ISO/IEC 27001:2022 ir susijusiems standartams bei vykdyti pareigas pagal taikomus teisės aktus ir reglamentavimo sistemas, tokias kaip ES BDAR, NIS2 direktyva, DORA reglamentas ir COBIT 2019.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas

4.1.1 Valdo šią politiką ir užtikrina jos taikymą visoje organizacijoje.

4.1.2 Peržiūri ir tvirtina visas formalias išimtis ir neatidėliotinos prieigos atvejus.

4.1.3 Teikia informaciją apie su paskyromis susijusias audito išvadas ir eskaluoja rizikas vadovybei.

4.2 Prieigos kontrolės vadovas / IT administratorius

4.2.1 Prižiūri ir valdo technines kontrolės priemones, skirtas naudotojų paskyrų gyvavimo ciklo valdymui.

4.2.2 Vykdo naudotojų prieigos suteikimo, panaikinimo ir privilegijų valdymo veiksmus pagal patvirtintas užklausas.

4.2.3 Tvarko patikimą visų naudotojų paskyrų, jų būsenos ir privilegijų lygių registrą.

4.2.4 Teikia pagalbą auditų ir atitikties peržiūrų metu, pateikdamas žurnalus ir veiklos ataskaitas.

[... 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 arba įvykus reikšmingiems pokyčiams, susijusiems su:

9.1.1 Organizacine struktūra ar verslo procesais

9.1.2 IT sistemomis, tapatybės platformomis ar prieigos metodais

9.1.3 Reglamentavimo ar sutartiniais reikalavimais, susijusiais su tapatybės ir prieigos valdymu

9.2 Vyriausiasis informacijos saugumo pareigūnas (CISO) kartu su prieigos kontrolės vadovu atsako už peržiūros proceso inicijavimą ir suinteresuotųjų šalių grįžtamojo ryšio koordinavimą.

9.3 Tarpinės peržiūros gali būti inicijuojamos dėl:

9.3.1 Saugumo incidentų, susijusių su netinkamu paskyrų naudojimu

9.3.2 Audito išvadų, atskleidžiančių paskyrų gyvavimo ciklo valdymo trūkumus

9.3.3 Naujų tapatybės ar privilegijuotos prieigos valdymo priemonių diegimo

9.4 Šios politikos atnaujinimai turi būti:

9.4.1 Valdomi taikant versijų kontrolę ir registruojami ISVS dokumentacijos bibliotekoje

9.4.2 Pateikiami visoms susijusioms suinteresuotosioms šalims, įskaitant padalinių vadovus, IT operacijų funkciją ir HR

9.4.3 Palaikomi atnaujinta mokymų medžiaga ir procedūrinėmis gairėmis

9.5 Visi pakeitimai turi būti patvirtinti vadovybės arba Informacijos saugumo valdymo komiteto ir registruojami audito tikslais.

10. Susijusios politikos ir sąsajos

10.1 Ši politika veiklos požiūriu yra susieta su toliau nurodytomis ISVS politikomis ir jomis palaikoma:

10.1.1 P4 Prieigos kontrolės politika: nustato bendruosius prieigos kontrolės principus ir mechanizmus, įskaitant taisyklėmis grindžiamas ir vaidmenimis grindžiamos prieigos kontrolės priemones.

10.1.2 P7 Įdarbinimo ir darbo santykių nutraukimo politika: nustato procedūrinius veiksmus naudotojų prieigai inicijuoti ir nutraukti, suderintus su HR veiksmais.

10.1.3 P8 Informacijos saugumo supratimo ir mokymo politika: stiprina naudotojų atsakomybę už paskyrų saugumą ir prisijungimo duomenų apsaugą.

10.1.4 P13 Duomenų klasifikavimo ir ženklinimo politika: nustato prieigos lygių gaires pagal duomenų klasifikaciją, užtikrindama, kad privilegijų ribos atitiktų jautrumo lygius.

10.1.5 P22 Žurnalų tvarkymo ir stebėsenos politika: užtikrina, kad audito pėdsakai būtų renkami visai su paskyromis susijusiai veiklai ir peržiūrimi siekiant nustatyti anomalijas ar neautorizuotą naudojimą.

10.1.6 P30 Reagavimo į incidentus politika: reglamentuoja eskalavimą, lokalizavimą ir veiksmus po incidento privilegijų netinkamo naudojimo ar neautorizuotos paskyrų veiklos atvejais.

10.2 Visos šios politikos kartu užtikrina nuoseklią, rizika grindžiamą tapatybės ir prieigos valdymo sistemą visoje organizacijoje.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika yra suderinta su pasauliniu mastu pripažintais kibernetinio saugumo standartais ir reglamentavimo sistemomis, pagal kurias saugus tapatybės, prieigos ir privilegijų valdymas yra esminė organizacijos informacijos saugumo dalis.

11.2 ISO/IEC 27001:

11.2.1 6.1.3 skyrius – reikalauja, kad organizacijos nustatytų, įvertintų ir tvarkytų informacijos saugumo rizikas, todėl prieigos ir privilegijų valdymas tampa formalia, rizika grindžiama kontrolės priemone, integruota į ISVS planavimo procesą.

11.2.2 8.1 skyrius – Veiklos planavimas ir kontrolė: sustiprina techninių ir procedūrinių apsaugos priemonių, reglamentuojančių naudotojų ir privilegijuotą prieigą, įgyvendinimą.

11.3 ISO/IEC 27002:2022 – kontrolės priemonės nuo 5.15 iki 5.18:

11.3.1 Kontrolės priemonė 5.15 – Naudotojų prieigos valdymas: remia formalius paskyrų suteikimo, prieigos autorizavimo ir periodinės prieigos teisių peržiūros procesus.

11.3.2 Kontrolės priemonė 5.16 – Tapatybės valdymas: nustato tapatybės unikalumo, gyvavimo ciklo kontrolės priemones ir saugaus autentifikavimo taikymą.

11.3.3 Kontrolės priemonė 5.17 – Autentifikavimo informacija: užtikrina, kad autentifikavimo informacijos paskirstymas ir valdymas būtų griežtai kontroliuojami, atsekami ir suderinti su mažiausių privilegijų principu per visą naudotojo paskyros gyvavimo ciklą.

11.3.4 Kontrolės priemonė 5.18 – Privilegijuotos prieigos teisės: įgyvendinama taikant vaidmenimis grindžiamą privilegijų priskyrimą, auditą ir padidintos prieigos tvirtinimo reikalavimus.

11.4 Šios kontrolės priemonės nustato struktūrizuoto paskyrų registravimo, išregistravimo, privilegijų atskyrimo ir autentifikavimo informacijos naudojimo gaires. Politika užtikrina tapatybės gyvavimo ciklo valdyseną, prieigą reikiamu laiku ir padidintų privilegijų sesijų stebėseną, kad būtų užkirstas kelias neautorizuotam sistemų naudojimui.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Prieigos kontrolės politika) ir AC-2 (Paskyrų valdymas): susieti su politikos reikalavimais dėl prieigos tvirtinimo, vaidmenų susiejimo ir naudotojų paskyrų audito.

11.5.2 AC-5 (Pareigų atskyrimas) ir AC-6 (Mažiausios privilegijos): įgyvendinami per privilegijų ribojimą, suderinimą su darbo vaidmenimis ir dvigubą patvirtinimą didelės rizikos užduotims.

11.5.3 IA-2–IA-5 (Identifikavimas ir autentifikavimas): užtikrinami taikant stipraus autentifikavimo mechanizmus, autentifikavimo duomenų gyvavimo ciklo taisykles ir MFA reikalavimus.

11.5.4 AU-2, AU-12 (audito žurnalų registravimas ir analizė): įgyvendinami per sesijų įrašymą ir privilegijuotos veiklos stebėseną jautriose aplinkose.

11.6 ES BDAR (2016/679):

11.6.1 32 straipsnis – Tvarkymo saugumas: reikalauja prieigos kontrolės priemonių ir tapatybės patikrinimo mechanizmų asmens duomenims apsaugoti. Tai įgyvendinama nustatant paskyrų tvirtinimo, privilegijų peržiūrų ir stipraus autentifikavimo apsaugos priemonių reikalavimus.

11.6.2 5 straipsnio 1 dalies f punktas – Vientisumas ir konfidencialumas: užtikrina, kad asmens duomenis galėtų pasiekti tik autorizuoti naudotojai, turintys teisėtą vaidmenį; tai sustiprinama taikant paskyrų valdymo kontrolės priemones.

11.6.3 39 konstatuojamoji dalis: reikalauja aiškaus prieigos ribojimo ir atskaitomybės – ši politika užtikrina visišką naudotojų tapatybių ir privilegijų priskyrimų atsekamumą.

11.7 ES NIS2 direktyva (2022/2555):

11.7.1 21 straipsnio 2 dalies a, d punktai: reikalauja, kad subjektai taikytų prieigos valdymo politikas ir užtikrintų saugų autentifikavimo duomenų bei privilegijuotų sesijų tvarkymą; tai palaikoma šios politikos naudotojų prieigos suteikimo, stebėsenos ir išimčių kontrolės priemonėmis.

11.7.2 21 straipsnio 3 dalis: skatina prieigos drausmę ir stiprų tapatybės užtikrinimą kritiniuose sektoriuose; tai įgyvendinama naudojant unikalius identifikatorius, RBAC ir laiko požiūriu apribotą padidintą prieigą.

11.8 ES DORA reglamentas (2022/2554):

11.8.1 5 straipsnis – IRT valdysena ir kontrolė: nustato formalizuotų IRT naudotojų valdymo procesų reikalavimą, kuris įgyvendinamas dokumentuotu suteikimu, išjungimu ir išimčių valdymu.

11.8.2 9 straipsnis – IRT rizikos valdymas: nustato organizacijoms pareigą apsaugoti sistemas taikant prieigos apribojimus ir stebėseną; tai įgyvendinama naudojant MFA, privilegijuotos prieigos žurnalavimą ir centralizuotas peržiūras.

11.9 COBIT 2019:

11.9.1 DSS01 – Valdomos operacijos: skatina standartizuotų veiklos kontrolės priemonių taikymą, įskaitant naudotojų paskyrų gyvavimo ciklo valdymą ir prieigos dokumentavimą.

11.9.2 DSS05 – Valdomos saugumo paslaugos: atspindi saugų naudotojų ir sistemų privilegijų administravimą, palaikant rizikos mažinimą taikant mažiausių privilegijų principą ir audito pėdsako patvirtinimą.

11.9.3 APO13 – Valdomas saugumas: reikalauja prieigos valdysenos skaitmeniniams ištekliams; tai įgyvendinama taikant formalizuotą paskyrų ir vaidmenų autorizavimo praktiką bei periodinių peržiūrų reikalavimus.