					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P11S					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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	5.3, 8 punktai	Vaidmenys, atsakomybės ir veiklos planavimas / kontrolė naudotojų prieigos valdymui
ISO/IEC 27002:2022	Kontrolė 8	Kontrolės priemonės privilegijų suteikimui, peržiūrai ir panaikinimui
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Paskyrų kūrimas, stebėsena, mažiausių privilegijų principas ir pareigų atskyrimas
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	Naudotojų prieigos valdymas esminiams ir svarbiems subjektams
ES DORA reglamentas	9 straipsnio 2 dalies b punktas	Privilegijuotos prieigos valdymas finansų subjektuose
COBIT 2019	DSS05.03, DSS05.04	Naudotojų prieigos suteikimas, prieigos panaikinimas ir periodinė peržiūra
ES BDAR	32 straipsnis	Tinkamos prieigos kontrolės priemonės asmens duomenų apsaugai

1. Tikslas

1.1 Ši politika nustato taisykles, kaip saugiai, nuosekliai ir užtikrinant atsekamumą valdyti naudotojų paskyras ir prieigos teises. Ji užtikrina, kad prieigą prie sistemų ir duomenų turėtų tik autorizuoti naudotojai ir kad suteikta prieiga atitiktų jų vaidmenį bei atsakomybes.

1.2 Veiksmingas paskyrų ir privilegijų valdymas yra būtinas siekiant užkirsti kelią neteisėtai prieigai, mažinti vidines grėsmes ir užtikrinti atitiktį ISO/IEC 27001, ES BDAR ir kitiems reglamentavimo reikalavimams.

1.3 Ši politika leidžia organizacijai priskirti paskyrų naudojimo savininkystę ir atsakomybę, stebėti bei audituoti privilegijų pakėlimus ir saugiai išjungti arba atšaukti prieigą, kai jos nebereikia.

1.4 Ji taip pat apsaugo veiklą nuo operacinių klaidų ar netinkamo naudojimo, kurį lemia perteklinė arba nestebima prieiga, ir padeda mažinti atsitiktinio duomenų nutekėjimo, netinkamo privilegijų naudojimo ar neatitikties reglamentavimo reikalavimams riziką.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems darbuotojams, praktikantams, rangovams ir trečiųjų šalių naudotojams, turintiems prieigą prie organizacijos IT sistemų.

2.1.2 Visoms sistemoms, įrenginiams, paslaugoms ir platformoms, kurias organizacija valdo pati arba kurios valdomos jos vardu, įskaitant debesijos platformas, vietinę infrastruktūrą ir trečiųjų šalių priemones.

2.2 Ji apima visų tipų naudotojų paskyras, įskaitant:

2.2.1 Vardines naudotojų paskyras (pvz., el. pašto paskyras, sistemų prisijungimus).

2.2.2 Administratoriaus ir sistemos lygmens paskyras.

2.2.3 Laikinas, svečio arba trečiųjų šalių prieigos paskyras.

2.2.4 Paslaugų paskyras, naudojamas taikomųjų programų arba automatizavimo sistemų.

2.3 Politika taikoma visam paskyros gyvavimo ciklui – nuo sukūrimo ir patvirtinimo iki keitimo, stebėsenos ir išjungimo. Tai apima pirminį naudotojų prieigos suteikimą įdarbinimo metu, prieigos peržiūras keičiantis vaidmenims ir prieigos teisių atšaukimą darbo santykių nutraukimo proceso metu.

3. Tikslai

3.1 Priskirti unikalias, atsekamas naudotojų tapatybes visiems sistemų naudotojams, užtikrinant atskaitomybę ir atsisakant priklausomybės nuo bendrų prisijungimo duomenų.

3.2 Taikyti mažiausių privilegijų principą, užtikrinant, kad naudotojams būtų suteikiamas tik minimalus prieigos lygis, būtinas jų pareigoms vykdyti.

3.3 Užkirsti kelią neautorizuotai prieigai prie jautrių sistemų ar duomenų taikant aiškiai dokumentuotas tvirtinimo ir peržiūros procedūras.

3.4 Užtikrinti savalaikį naudotojų paskyrų išjungimą, kai jų nebereikia, pvz., nutraukus darbo santykius, pasibaigus sutarčiai arba pasikeitus vaidmeniui.

3.5 Palaikyti saugią, auditui parengtą aplinką dokumentuojant visus paskyrų pakeitimus, patvirtinimus ir periodines peržiūras.

3.6 Užtikrinti, kad privilegijų pakėlimas būtų griežtai kontroliuojamas, tvirtinamas nepriklausomai ir registruojamas žurnaluose, o padidintos prieigos teisės būtų nedelsiant panaikinamos, kai jų nebereikia.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 Atsako už bendrą šios politikos taikymą.

4.1.2 Užtikrina, kad paskyrų valdymo praktika atitiktų ISO/IEC 27001 sertifikavimo reikalavimus ir taikomus teisinius įpareigojimus (pvz., ES BDAR).

4.1.3 Turi būti nedelsiant informuojamas apie bet kokią neteisėtą prieigą, saugumo incidentą ar politikos pažeidimą, susijusį su naudotojų paskyromis.

4.1.4 Prižiūri politikos peržiūras, auditus ir politikos vykdymo užtikrinimo veiksmus.

4.2 IT vadovas arba išorinis IT paslaugų teikėjas

4.2.1 Atsako už techninį paskyrų ir privilegijų kontrolės priemonių įgyvendinimą visose organizacijos naudojamose sistemose.

4.2.2 Turi suteikti, keisti ir išjungti naudotojų paskyras tik pagal dokumentuotus patvirtinimus.

4.2.3 Turi užtikrinti slaptažodžių sudėtingumo reikalavimus, ekrano užrakinimo laiką, kelių veiksnių autentifikavimą (jei prieinamas) ir sistemų žurnalavimą.

4.2.4 Turi tvarkyti saugius visų prieigos patvirtinimų, paskyrų savininkystės, privilegijų pakėlimų ir prieigos teisių atšaukimo įrašus.

4.2.5 Privalo stebėti neautorizuotas ar našlaičių paskyras ir apie neatitikimus pranešti GM.

[... 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 GM ir IT vadovo, siekiant užtikrinti atitiktį:

9.1.1 Galiojančioms ISO/IEC 27001:2022 kontrolės priemonėms ir gairėms

9.1.2 Reglamentavimo pokyčiams (pvz., ES BDAR, DORA, NIS2)

9.1.3 Sistemų, paslaugų arba verslo struktūros pokyčiams

9.2 Peržiūros taip pat turi būti atliekamos po:

9.2.1 Reikšmingų saugumo incidentų arba audito išvadų

9.2.2 Esminių IT sistemų arba paskyrų architektūros pokyčių

9.2.3 Naujų platformų, kurioms reikalinga prieigos kontrolės integracija, įdiegimo

9.3 Visi pakeitimai turi būti patvirtinti GM ir aiškiai komunikuoti paveiktam personalui.

10. Susijusios politikos ir sąsajos

10.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atskaitomybę ir sprendimų priėmimo įgaliojimus dėl prieigos tvirtinimo ir priežiūros.

10.2 P4S – Prieigos kontrolės politika: reglamentuoja visos sistemos mastu taikomą prieigos kontrolę ir autentifikavimo metodus.

10.3 P7S – Įdarbinimo ir darbo santykių nutraukimo politika: užtikrina, kad paskyrų kūrimas ir panaikinimas būtų įtraukti į žmogiškųjų išteklių valdomus personalo pokyčius.

10.4 P8S – Informacijos saugumo supratimo ir mokymo politika: moko naudotojus saugios paskyrų naudojimo praktikos ir nustato naudojimo lūkesčius.

10.5 P30S – Reagavimo į incidentus politika: apibrėžia veiksmus, kurių reikia imtis, jei dėl netinkamo paskyros naudojimo įvyksta saugumo pažeidimas arba neautorizuotas atskleidimas.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 5.3 punktas: reikalauja, kad informacijos saugumo vaidmenys ir atsakomybės būtų aiškiai priskirti ir taikomi.

11.1.2 8.1 punktas: veiklos planavimas ir kontrolė turi apimti naudotojų prieigos valdymą.

11.2 ISO/IEC 27002

11.2.1 Kontrolė 8.2: apibrėžia technines ir procedūrines kontrolės priemones padidintų privilegijų suteikimui, peržiūrai ir panaikinimui.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: reikalauja paskyrų kūrimo, stebėsenos ir atšaukimo pagal nustatytus vaidmenis ir procesus.

11.3.2 AC-5: apima pareigų atskyrimą siekiant išvengti konflikto arba piktnaudžiavimo privilegijomis.

11.3.3 AC-6: nustato pareigą taikyti mažiausių privilegijų principą visoms prieigos teisėms.

11.4 ES BDAR

11.4.1 32 straipsnis: reikalauja taikyti tinkamas prieigos kontrolės priemones, kad asmens duomenys būtų apsaugoti nuo neteisėtos prieigos arba pakeitimo.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies d punktas: nustato naudotojų prieigos valdymą kaip vieną iš pagrindinių saugumo kontrolės priemonių esminiams ir svarbiems subjektams.

11.6 ES DORA reglamentas

11.6.1 9 straipsnio 2 dalies b punktas: reikalauja, kad finansų subjektai įgyvendintų prieigos kontrolės priemones, ribojančias ir stebinčias privilegijuotas teises.

11.7 COBIT 2019

11.7.1 DSS05.03: nustato naudotojų prieigos suteikimą ir prieigos panaikinimą kaip IT valdysenos dalį.

11.7.2 DSS05.04: numato nuolatinę naudotojų prieigos peržiūrą ir jos derinimą su organizaciniais vaidmenimis.