					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P07					Dokumento pavadinimas: **Įdarbinimo ir darbo santykių nutraukimo 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	Pastaba
ISO/IEC 27001:2022	7.2 skyrius, 6 skyrius	Personalo kompetencija, saugi integracija ir atsakomybių, susijusių su darbo santykių nutraukimu ar pakeitimu, įgyvendinimas.
ISO/IEC 27002:2022	Kontrolės priemonės 6.2, 6.5, 5	Įdarbinimo, prieigos ir personalo gyvavimo ciklo kontrolės priemonės.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Personalo perkėlimas ir darbo santykių nutraukimas, mažiausių privilegijų principas, audito žurnalų registravimas, prieigos valdymas personalo pokyčių metu ir po jų.
ES BDAR	5 straipsnio 1 dalies f punktas, 25, 32 straipsniai; 39 konstatuojamoji dalis	Prieigos ribojimas, konfidencialumas, apsauga ir tinkamos personalo duomenų kontrolės priemonės.
ES NIS2 direktyva	21 straipsnio 2 dalies b, c, d punktai	Personalo ir operacinio saugumo priemonės, vidinių grėsmių mažinimas, gyvavimo ciklo procesai.
ES DORA reglamentas	5, 8, 9 straipsniai	Valdysena, vidaus IRT kontrolė, IRT rizika, incidentų valdymas personalo perkėlimo laikotarpiu.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Žmogiškieji ištekliai, žinių valdymas, saugumas ir atitiktis įdarbinimo bei darbo santykių nutraukimo metu.

1. Tikslas

1.1 Ši politika nustato standartizuotas procedūras, skirtas valdyti įdarbinimą, vidinius perkėlimus ir darbo santykių nutraukimą visų tipų naudotojams.

1.2 Ji užtikrina savalaikį ir saugų fizinės bei loginės prieigos teisių suteikimą ir panaikinimą, kartu užtikrinant konfidencialumą, atskaitomybę ir turto grąžinimą.

1.3 Ši politika mažina riziką, susijusią su neautorizuota prieiga, duomenų nutekėjimu ir negrąžintu turtu, integruodama įdarbinimo ir darbo santykių nutraukimo kontrolės priemones į žmogiškųjų išteklių, IT ir saugumo procesus.

1.4 Ši politika padeda įgyvendinti ISO/IEC 27001:2022 A priedo 6.5 kontrolės priemonės reikalavimus, užtikrindama, kad personalo saugumo įpareigojimai būtų taikomi darbo santykių ar bendradarbiavimo metu ir po jų.

2. Taikymo sritis

2.1 Ši politika taikoma visiems darbuotojams, rangovams, konsultantams, tiekėjams ir kitoms trečiosioms šalims, kurioms suteikta prieiga prie organizacijos sistemų, tinklų, patalpų ar duomenų.

2.2 Ji reglamentuoja visą toliau nurodytą gyvavimo ciklą:

2.2.1 įvedimą į darbą (įdarbinimą, sutarties sudarymą arba laikiną įtraukimą)

2.2.2 vidinius perkėlimus arba pareigų pasikeitimą

2.2.3 darbo santykių nutraukimo procesą (atsistatydinimą, išėjimą į pensiją, atleidimą, sutarties galiojimo pabaigą)

2.3 Politika apima:

2.3.1 loginę prieigą (sistemas, taikomąsias programas, debesijos paslaugas, virtualųjį privatųjį tinklą (VPN))

2.3.2 fizinę prieigą (korteles, raktus, patekimo į pastatą sistemas)

2.3.3 priskirtą turtą (nešiojamuosius kompiuterius, telefonus, žetonus, prisijungimo duomenis)

2.3.4 susipažinimo su politikomis patvirtinimą ir konfidencialumo įsipareigojimus

2.4 Visi padaliniai (žmogiškųjų išteklių, IT, patalpų valdymo, saugumo ir vadovybės) atsako už savo vaidmens vykdymą įvedimo į darbą ir darbo santykių nutraukimo procesuose.

3. Tikslai

3.1 Užtikrinti, kad visam personalui prieiga būtų suteikiama tik įvykdžius saugumo, mokymų ir sutartines išankstines sąlygas.

3.2 Panaikinti prieigos teises ir susigrąžinti organizacijos turtą nedelsiant pasikeitus pareigoms arba nutrūkus darbo santykiams.

3.3 Išsaugoti organizacijos turto konfidencialumą, vientisumą ir prieinamumą personalo pokyčių metu.

3.4 Užtikrinti audituojamumą ir galimybę pagrįsti veiksmus teisiniu požiūriu, kaupiant išsamius įdarbinimo ir darbo santykių nutraukimo įrašus.

3.5 Mažinti vidinių grėsmių poveikį, tikrinant ir dokumentuojant visus su personalu susijusius prieigos įvykius.

3.6 Suderinti organizacijos personalo gyvavimo ciklą su rizika grindžiamomis saugumo praktikomis ir reglamentavimo reikalavimais.

4. Vaidmenys ir atsakomybės

4.1 Vykdomoji vadovybė

4.1.1 Tvirtina šią politiką ir skiria įgaliojimus bei išteklius įdarbinimo, darbo santykių nutraukimo ir prieigos kontrolės procesams.

4.1.2 Užtikrina, kad personalo pokyčiai nesukeltų organizacijai nepagrįstos saugumo ar teisinės rizikos.

4.2 Žmogiškieji ištekliai (HR)

4.2.1 Inicijuoja darbuotojų įvedimo į darbą ir darbo santykių nutraukimo darbo srautus bei informuoja susijusius padalinius apie pokyčius.

4.2.2 Užtikrina, kad asmens patikimumo patikrinimai, sutartys, konfidencialumo susitarimai ir susipažinimo su politikomis patvirtinimai būtų užbaigti prieš suteikiant prieigą.

4.2.3 Informuoja IT ir patalpų bei turto valdymo padalinius apie darbuotojų išėjimą pagal pranešimų paslaugų lygio susitarimą.

4.2.4 Koordinuoja veiksmus su teisės padaliniu, kad būtų užtikrinti įsipareigojimai po darbo santykių pabaigos (pvz., konfidencialumo sąlygos).

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Politikos peržiūros dažnumas

9.1.1 Ši politika turi būti peržiūrima:

9.1.1.1 kasmet, arba

9.1.1.2 po bet kokio esminio incidento, susijusio su netinkamu prieigos naudojimu, turto praradimu ar procedūrų nesuveikimu

9.1.1.3 įgyvendinus esminius žmogiškųjų išteklių ar IAM platformos pakeitimus

9.1.1.4 pasikeitus reglamentavimo ar teisiniams reikalavimams, turintiems įtakos personalo duomenims ar įpareigojimams

9.2 Peržiūros procesas ir atsakomybė

9.2.1 ISVS vadovas ir Žmogiškųjų išteklių direktorius koordinuoja peržiūrą, įtraukdami IT saugumą, teisės padalinį ir atitikties funkciją.

9.2.2 Visi pakeitimai turi būti patvirtinti vykdomosios vadovybės ir ISVS valdymo komiteto.

9.2.3 Atnaujintos versijos turi būti pakartotinai išplatintos susijusiems padaliniams ir darbuotojams, kad jie iš naujo patvirtintų susipažinimą.

9.3 Dokumentų kontrolė ir saugojimas

9.3.1 Šioje politikoje turi būti nurodyta:

9.3.2 versijų valdymas, versijų istorija ir įsigaliojimo data

9.3.3 atsakingas savininkas ir peržiūrintys asmenys

9.3.4 politikos klasifikacija ir patvirtinimo įrašas

9.3.5 Nebegaliojančios versijos turi būti archyvuojamos ne trumpiau kaip 3 metus pagal Dokumentų valdymo politiką.

10. Susijusios politikos ir sąsajos

10.1.1 Ši politika tiesiogiai integruojama su:

10.1.2 P1 – Informacijos saugumo politika: nustato organizacijos saugumo tikslus, įskaitant personalo prieigos valdyseną.

10.1.3 P4 – Prieigos kontrolės politika: nustato operacinius reikalavimus sistemų ir fizinės prieigos teisių suteikimui ir panaikinimui pagal įvedimo į darbą ir darbo santykių nutraukimo paleidiklius.

10.1.4 P3 – Priimtino naudojimo politika: reikalauja patvirtinimo įvedimo į darbą metu ir palaiko politikos taikymą po darbo santykių nutraukimo.

10.1.5 P6 – Rizikos valdymo politika: užtikrina, kad naudotojų prieigos ir perėjimo rizikos būtų vertinamos ir mažinamos laikantis ISVS principų.

10.1.6 P11 – Naudotojų paskyrų ir privilegijų valdymo politika: reglamentuoja technines kontrolės priemones prieigos suteikimui ir prieigos teisių panaikinimui pagal šią politiką.

10.2 Šios politikos sudaro integruotą kontrolės sistemą, skirtą saugiai ir atskaitingai valdyti su personalo gyvavimo ciklu susijusius įvykius.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintomis saugumo, privatumo ir IT valdysenos sistemomis, siekiant užtikrinti, kad įdarbinimo ir darbo santykių nutraukimo procesai būtų saugūs, atsekami ir atitiktų teisinius bei organizacinius reikalavimus.

11.2 ISO/IEC 27001:

11.2.1 7.2 skyrius – Kompetencija ir 6.2 skyrius – Informacijos saugumo tikslai: ši politika padeda užtikrinti personalo kompetenciją ir saugią asmenų integraciją į vaidmenis, kurie daro įtaką ISVS tikslams.

11.2.2 A priedo 6.5 kontrolės priemonė – Atsakomybės po darbo santykių nutraukimo arba darbo pobūdžio pakeitimo: ši politika visapusiškai užtikrina likutinių prieigos teisių, duomenų globos ir sutartinių įpareigojimų kontrolę išėjimo metu.

11.2.3 A priedo 5.9 kontrolės priemonė – Tikrinimas ir 6.2 kontrolės priemonė – Darbo sąlygos: įvedimo į darbą procedūros apima asmens patikimumo patikrinimą ir susipažinimo su politika patvirtinimo mechanizmus, atitinkančius šiuos reikalavimus.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (darbo santykių nutraukimas) ir PS-5 (personalo perkėlimas): ši politika užtikrina struktūruotą prieigos teisių, fizinių kortelių ir turto panaikinimą arba pakeitimą.

11.3.2 AC-2 (paskyrų valdymas) ir AC-6 (mažiausių privilegijų principas): nustatyta, kad prieiga turi atitikti vaidmenį ir būti nedelsiant atšaukta, kai jos nebereikia.

11.3.3 IA-4 (identifikatorių valdymas) ir IA-5 (autentifikatorių valdymas): palaikomas saugus prisijungimo duomenų valdymas personalo pokyčių metu ir po jų.

11.3.4 CM-5 (prieigos apribojimai keičiant): užkerta kelią neautorizuotiems pakeitimams po darbo santykių nutraukimo, panaikinant padidintas prieigos teises.

11.3.5 AU-2 ir AU-6: prieigos įvykių žurnalai ir atsekamumas stiprinami integruojant IAM ir audito pėdsaką.

11.4 ES BDAR (2016/679):

11.4.1 5 straipsnio 1 dalies f punktas: saugo asmens duomenis nuo neautorizuotos prieigos; šioje politikoje tai užtikrinama panaikinant naudotojų prieigą darbo santykių nutraukimo metu.

11.4.2 32 straipsnis: reikalauja taikyti tinkamas technines ir organizacines kontrolės priemones asmens duomenų saugumui viso darbo santykių gyvavimo ciklo metu.

11.4.3 25 straipsnis – Duomenų apsauga pagal projektavimą: užtikrina, kad įdarbinimo ir darbo santykių nutraukimo procesuose būtų integruotas duomenų minimizavimas, saugojimas ir teisėta prieigos kontrolė.

11.4.4 39 konstatuojamoji dalis: pabrėžia prieigos ribojimą ir konfidencialumą, kuriuos palaiko šios politikos struktūra.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 21 straipsnio 2 dalies b, c, d punktai: reikalauja taikyti personalo ir operacinio saugumo priemones prieigos kontrolei, vidinių grėsmių mažinimui ir gyvavimo ciklo procesams, kurie visi atspindėti šioje politikoje.

11.6 ES DORA reglamentas (2022/2554):

11.6.1 5 straipsnis – Valdysena ir vidaus kontrolė: ši politika remia vidaus IRT valdyseną, susijusią su žmogiškąja rizika ir prieigos valdymu.

11.6.2 8 straipsnis – IRT rizikos valdymas: taiko kontrolės priemones personalo pokyčiams, kurie gali lemti kritinio turto ar reguliuojamų aplinkų riziką.

11.6.3 9 straipsnis – Incidentų klasifikavimas ir valdymas: užtikrina, kad su darbo santykių nutraukimu susiję pažeidimai būtų registruojami ir mažinami taikant tinkamą prieigos teisių panaikinimą ir turto tvarkymą.

11.7 COBIT 2019:

11.7.1 APO07 – Valdomi žmogiškieji ištekliai: apibrėžia vaidmenis, atsakomybes ir gyvavimo ciklo veiksmus įdarbinimo bei darbo santykių nutraukimo srityje, suderintus su valdysenos tikslais.

11.7.2 BAI08 – Žinių valdymas: sustiprina procedūrų dokumentavimą, žinių išsaugojimą ir kontrolės perdavimą darbo santykių pabaigoje.

11.7.3 DSS05 – Valdomos saugumo paslaugos: užtikrina naudotojų išjungimą, turto kontrolę ir atskaitomybę keičiantis vaidmenims.

11.7.4 MEA03 – Atitikties stebėsena, vertinimas ir įvertinimas: užtikrina, kad įdarbinimo ir darbo santykių nutraukimo kontrolės priemonės būtų vertinamos vidaus ir išorės auditų metu.