					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P07S					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 reglamentavimo reikalavimais

Standartas / reglamentavimas	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	6.2, 7 skyriai	Žmogiškųjų išteklių saugumo ir informuotumo reikalavimai
ISO/IEC 27002:2022	Kontrolės priemonės 6.2, 6.5	Įdarbinimo ir darbo santykių nutraukimo saugumo praktika
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Darbo santykių nutraukimas; paskyrų gyvavimo ciklas; planavimas
ES NIS2 direktyva	21 straipsnio 2 dalies h punktas	Žmogiškųjų išteklių saugumas ir prieigos gyvavimo ciklas
ES DORA reglamentas	12 straipsnis	Prieigos kontrolė ir prieigos teisių atšaukimas IRT sistemose
COBIT 2019	APO07, DSS01	Darbuotojų saugumas, loginės ir fizinės prieigos kontrolės priemonės
ES BDAR	32 straipsnis	Asmens duomenų saugumas darbo santykių metu

1. Tikslas

1.1 Ši politika nustato naujų darbuotojų ir rangovų priėmimo procesą bei saugų prieigos panaikinimą, kai asmenys palieka organizaciją arba keičia pareigas.

1.2 Ja užtikrinama, kad prieiga būtų suteikiama laikantis mažiausių būtinų teisių principo, visas turtas būtų apskaitytas, o kritiniai veiksmai, tokie kaip sistemų išjungimas ir duomenų atkūrimas, būtų atlikti laiku.

1.3 Ši politika padeda užtikrinti atitiktį, veiklos tęstinumą ir duomenų apsaugą, nustatydama struktūruotas ir audituojamas priėmimo, perkėlimo ir darbo santykių nutraukimo veiklas.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems nuolatiniams ir laikiniesiems darbuotojams;

2.1.2 rangovams, konsultantams ir praktikantams;

2.1.3 išorės paslaugų teikėjams, turintiems sisteminę arba fizinę prieigą.

2.2 Ji apima:

2.2.1 priėmimą į darbą: naudotojų paskyrų sukūrimą, prieigos suteikimą, įrangos išdavimą;

2.2.2 darbo santykių nutraukimo procesą: prieigos panaikinimą, organizacijos turto susigrąžinimą ir saugų skaitmeninių tapatybių uždarymą;

2.2.3 vidinius pareigų pokyčius, kai reikia perkonfigūruoti prieigą arba iš naujo priskirti turtą.

2.3 Politika taikoma visiems įrenginiams, platformoms ir vietoms, naudojamiems oficialioms veiklos funkcijoms vykdyti.

3. Tikslai

3.1 Užtikrinti, kad nauji darbuotojai gautų prieigą ir išteklius pagal patvirtintus vaidmenis ir atsakomybes.

3.2 Užtikrinti, kad išeinantys naudotojai iki paskutinės darbo dienos pabaigos būtų visiškai pašalinti iš sistemų ir patalpų.

3.3 Užkirsti kelią bešeimininkėms paskyroms ir negrąžintam turtui, keliančiam saugumo riziką.

3.4 Išlaikyti dokumentuotus priėmimo, perkėlimo ir darbo santykių nutraukimo veiksmų įrašus.

3.5 Stiprinti atskaitomybę naudojant kontrolinius sąrašus ir užtikrinant tarpdisciplininį vaidmenų koordinavimą.

4. Vaidmenys ir atsakomybės

4.1 Bendrovės vadovas

4.1.1 Tvirtina prieigą didelių privilegijų vaidmenims ir prižiūri priėmimo bei darbo santykių nutraukimo procesą.

4.1.2 Užtikrina, kad išimtys būtų pagrįstos ir kad, nesilaikant proceso, būtų taikomi korekciniai veiksmai.

4.2 Biuro vadovas / žmogiškųjų išteklių funkcija

4.2.1 Inicijuoja naujų darbuotojų priėmimą į darbą ir informuoja IT apie išėjimus.

4.2.2 Užtikrina teisinių dokumentų įforminimą (pvz., konfidencialumo susitarimų) ir susipažinimo su saugumo politikomis patvirtinimų surinkimą.

4.2.3 Prižiūri priėmimo ir atleidimo kontrolinius sąrašus bei stebi politikos laikymąsi.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Metinė peržiūra

9.1.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus bendrovės vadovo ir žmogiškųjų išteklių / IT vadovų.

9.2 Ankstyvos peržiūros inicijavimo atvejai

9.2.1 Atnaujinimai turi būti atliekami, jei:

9.2.1.1 įdiegiamos naujos žmogiškųjų išteklių arba IT sistemos;

9.2.1.2 pasikeičia išorės IT paslaugų teikėjas arba valdoma žmogiškųjų išteklių paslauga;

9.2.1.3 saugumo auditai atskleidžia proceso spragas;

9.2.1.4 pasikeičia reglamentavimo įpareigojimai (pvz., ES BDAR atnaujinimai);

9.2.1.5 įvyksta kritinis darbo santykių nutraukimo proceso nesuveikimas arba pažeidimas.

9.3 Versijų valdymas ir tvirtinimas

9.3.1 Kiekvienoje šios politikos versijoje turi būti:

9.3.1.1 versijos numeris ir data;

9.3.1.2 pakeitimų santrauka;

9.3.1.3 bendrovės vadovo patvirtinimas;

9.3.1.4 mažiausiai trejus metus saugomas ankstesnių versijų archyvas.

9.4 Komunikacija ir patvirtinimas

9.4.1 Visi darbuotojai, atsakingi už įdarbinimą arba darbo santykių nutraukimą, turi būti informuojami apie visus politikos atnaujinimus. Metiniai informuotumo didinimo arba žinių atnaujinimo instruktažai yra privalomi.

10. Susijusios politikos ir sąsajos

10.1 Ši politika palaiko toliau nurodytas politikas ir yra jų palaikoma:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: užtikrina atskaitomybę prieigos ir įdarbinimo procesuose;

10.1.2 P4S – Prieigos kontrolės politika: nustato techninį vaidmenimis grindžiamos naudotojų prieigos suteikimo ir išjungimo įgyvendinimą;

10.1.3 P6S – Rizikos valdymo politika: vertina rizikas, kylančias dėl priėmimo į darbą ir darbo santykių nutraukimo kontrolės priemonių nesuveikimo;

10.1.4 P8S – Informacijos saugumo supratimo ir mokymo politika: nustato darbuotojų supažindinimo reikalavimus priėmimo į darbą metu;

10.1.5 P30S – Reagavimo į incidentus politika: prieigos teisių nepanaikinimą arba turto vagystę vertina kaip saugumo incidentus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.2 skyrius – nustato žmogiškųjų išteklių saugumo reikalavimus.

11.1.2 7.2 skyrius – nustato privalomus informuotumo mokymus naujiems darbuotojams.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonės 6.2 ir 6.5 – detalizuoja įdarbinimo ir darbo santykių nutraukimo saugumo praktikas.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – darbuotojų darbo santykių nutraukimo procedūros, įskaitant prieigos išjungimą.

11.3.2 AC-2 – užtikrina paskyrų gyvavimo ciklo valdymą naudotojų prieigai.

11.3.3 PL-4 – reikalauja planuoti darbuotojų perėjimus.

11.4 ES BDAR

11.4.1 32 straipsnis – užtikrina tinkamą saugumą darbo santykių metu ir jiems pasibaigus, ypač asmens duomenų prieigai.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies h punktas – reikalauja žmogiškųjų išteklių saugumo ir prieigos gyvavimo ciklo kontrolės priemonių.

11.6 ES DORA reglamentas

11.6.1 12 straipsnis – reikalauja, kad reguliuojami finansų subjektai kontroliuotų darbuotojų prieigą prie IRT sistemų, įskaitant prieigos teisių atšaukimo procedūras.

11.7 COBIT 2019

11.7.1 APO07 – Žmogiškųjų išteklių valdymas: nustato darbuotojų gyvavimo ciklo saugumo reikalavimus.

11.7.2 DSS01 – Operacijų valdymas: apima loginės ir fizinės prieigos kontrolę darbo santykių pokyčių metu.