					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P09S					Dokumento pavadinimas: **Nuotolinio darbo 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, 6.2, 8 skyriai	
ISO/IEC 27002:2022	Kontrolė 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
ES NIS2 direktyva	21 straipsnio 2 dalies b ir h punktai	ES NIS2
ES DORA reglamentas	9 straipsnis	ES DORA
COBIT 2019	DSS05, APO13	COBIT 2019
ES BDAR	32 straipsnis	ES BDAR

1. Tikslas

1.1 Ši politika nustato saugumo reikalavimus darbuotojams ir rangovams, dirbantiems nuotoliniu būdu, įskaitant darbą iš namų, bendradarbystės erdvėse ar kelionių metu.

1.2 Ja siekiama apsaugoti verslo informacijos, prie kurios jungiamasi ne organizacijos kontroliuojamoje aplinkoje, konfidencialumą, vientisumą ir prieinamumą.

1.3 Ši politika užtikrina atitiktį tarptautiniams standartams ir mažina tokias rizikas kaip neleistina prieiga, duomenų praradimas ir paslaugų sutrikimai.

2. Taikymo sritis

2.1 Ši politika taikoma visiems darbuotojams (darbuotojams, rangovams, konsultantams ir laikiniesiems darbuotojams), kurie, dirbdami ne organizacijos patalpose, jungiasi prie organizacijos sistemų, tinklų ar duomenų.

2.2 Ji apima:

2.2.1 organizacijos suteiktų ir asmeninių įrenginių naudojimą

2.2.2 prieigą per VPN, nuotolinį darbalaukį ar debesijos paslaugas

2.2.3 saugų informacijos tvarkymą už organizacijos patalpų ribų

2.2.4 stebėseną, išimčių valdymą ir politikos laikymosi užtikrinimą

2.3 Ji taikoma tiek nuolatiniam, tiek daliniam nuotoliniam darbui, įskaitant ad hoc nuotolinę prieigą.

3. Tikslai

3.1 Užkirsti kelią neleistinai prieigai prie organizacijos sistemų ar jautrių duomenų nuotolinio darbo metu.

3.2 Užtikrinti, kad už biuro ribų naudojami įrenginiai ir ryšio kanalai atitiktų bazinę konfigūraciją ir kitus minimalius saugumo reikalavimus.

3.3 Užtikrinti nuotolinės prieigos teisių valdymą ir stebėseną.

3.4 Pateikti darbuotojams ir vadovams aiškias gaires dėl saugaus nuotolinio darbo praktikos.

3.5 Užtikrinti atitiktį ISO, NIS2, BDAR, DORA ir COBIT reikalavimams, taikomiems nuotoliniam ir mobiliam darbui.

4. Vaidmenys ir atsakomybės

4.1 Generalinis direktorius

4.1.1 Tvirtina nuotolinio darbo susitarimus ir prižiūri atitiktį.

4.1.2 Eskaluoja saugumo incidentus arba pasikartojančius neatitikties atvejus.

4.1.3 Peržiūri išimtis ir užtikrina tolesnius veiksmus po incidentų.

4.2 IT pagalba arba išorinis IT paslaugų teikėjas

4.2.1 Įdiegia saugią nuotolinę prieigą (pvz., VPN, MFA).

4.2.2 Užtikrina galinių įrenginių saugumą, šifravimą ir įrenginių konfigūraciją.

4.2.3 Teikia pagalbą naudotojams ir tiria techninius saugumo klausimus.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Kasmetinė politikos peržiūra

9.1.1 Generalinis direktorius ir IT pagalba privalo kasmet peržiūrėti šią politiką, kad ji atitiktų technologinius, darbo organizavimo ir teisinius pokyčius.

9.2 Ankstyvo atnaujinimo priežastys

9.2.1 Nedelsiant atliekama peržiūra po:

9.2.1.1 didelio nuotolinio darbo saugumo incidento

9.2.1.2 NIS2, BDAR ar DORA reikalavimų pakeitimų

9.2.1.3 perėjimo prie naujos nuotolinės prieigos technologijos (pvz., kitos VPN platformos)

9.3 Versijų valdymas ir archyvavimas

9.3.1 Visos šios politikos versijos turi būti:

9.3.1.1 datuotos ir patvirtintos generalinio direktoriaus

9.3.1.2 sunumeruotos pagal versijas

9.3.1.3 archyvuojamos mažiausiai trejus metus

9.4 Informavimas darbuotojams

9.4.1 Apie politikos atnaujinimus turi būti informuoti visi nuotoliniai naudotojai. Bet kuriam reikšmingam pakeitimui būtinas patvirtinimas.

10. Susijusios politikos ir sąsajos

10.1 Ši politika siejama su šiomis politikomis ir jas papildo:

10.1.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: apibrėžia, kas suteikia leidimą nuotolinei prieigai ir vykdo jos priežiūrą

10.1.2 P4S – Prieigos kontrolės politika: nustato saugios nuotolinės prieigos įdiegimo ir panaikinimo procedūras

10.1.3 P6S – Rizikos valdymo politika: nustato rizikų, susijusių su prieiga ne organizacijos patalpose, stebėseną ir vertinimą

10.1.4 P8S – Informacijos saugumo informuotumo ir mokymo politika: moko naudotojus apie nuotolinio darbo rizikas ir gerąją praktiką

10.1.5 P30S – Reagavimo į incidentus politika: reglamentuoja reagavimą į nuotolinės prieigos incidentus, tokius kaip prisijungimo duomenų nutekėjimas ar įrenginio praradimas

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 6.1 skyrius – rizika grindžiamas planavimas nuotolinės prieigos scenarijams

11.1.2 6.2 skyrius – apibrėžia žmogiškųjų išteklių atsakomybes mobiliojo ir nuotolinio darbo kontekste

11.1.3 8 skyrius – nuotolinių procesų operacinis planavimas ir kontrolė

11.2 ISO/IEC 27002

11.2.1 Kontrolė 6.7 – pateikia praktines gaires dėl nuotolinio ir mobiliojo darbo saugumo

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – nuotolinės prieigos kontrolė, sesijų apsauga ir saugumo stebėsena

11.3.2 AC-2 – paskyrų kontrolė ne organizacijos patalpose dirbantiems naudotojams

11.4 ES BDAR

11.4.1 32 straipsnis – reikalauja duomenų apsaugos pagal projektavimą ir pagal numatytuosius nustatymus, įskaitant nuotolinio darbo aplinką

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies b punktas – reikalauja saugaus tinklų ir informacinių sistemų naudojimo

11.5.2 21 straipsnio 2 dalies h punktas – numato su žmogiškaisiais ištekliais susijusias saugumo priemones, įskaitant kontrolės priemones dirbant ne organizacijos patalpose

11.6 ES DORA reglamentas

11.6.1 9 straipsnis – reikalauja, kad finansų subjektai užtikrintų IRT atsparumą visais veiklos režimais, įskaitant nuotolinę prieigą

11.7 COBIT 2019

11.7.1 DSS05 – saugumo paslaugų valdymas: apima galinių įrenginių apsaugą ir saugaus nuotolinio darbo praktiką

11.7.2 APO13 – valdomas saugumas: užtikrina saugų mobiliosios ir nuotolinės prieigos suteikimą bei rizikos priežiūrą