| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Čia įrašykite registruoto juridinio asmens pavadinimą | | | | | | | |
| Dokumento numeris:<br>P09 | | | | | Dokumento pavadinimas:<br>**Nuotolinio darbo politika** | | | | | | | |
| Versija:<br>1.0 | | Įsigaliojimo data:<br>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** |
| | | | |
| | | | |

**Teisinis pranešimas (autorių teisės ir naudojimo apribojimai)**

(C) 2025 Clarysec LLC. All rights reserved.

Šis dokumentas yra Clarysec LLC intelektinė nuosavybė. Jokia šio dokumento dalis negali būti kopijuojama, pakartotinai naudojama, platinama ar keičiama komerciniais ar įgyvendinimo tikslais be išankstinio aiškaus rašytinio leidimo.

Neautorizuotas naudojimas yra griežtai draudžiamas ir gali užtraukti teisinius veiksmus.

Dėl licencijavimo kreipkitės: info@clarysec.com

## 1. Tikslas

1.1 Ši politika nustato privalomuosius reikalavimus saugiam nuotolinio darbo vykdymui, įskaitant organizacijos sistemų naudojimą, prieigą prie duomenų ir darbo pareigų vykdymą už organizacijos patalpų ribų.

1.2 Ji užtikrina nuotoliniu būdu pasiekiamų informacijos išteklių konfidencialumą, vientisumą ir prieinamumą bei nustato kontrolės priemones, skirtas mažinti su paskirstytomis darbo aplinkomis susijusią riziką.

1.3 Ši politika įgyvendina ISO/IEC 27001:2022 A priedo kontrolę 6.7, taikydama technines ir procedūrines apsaugos priemones, pritaikytas nuotolinio darbo sąlygoms.

## 2. Taikymo sritis

**2.1 Ši politika taikoma visam personalui, kuriam suteiktas leidimas dirbti nuotoliniu būdu, įskaitant:**

2.1.1 darbuotojus (dirbančius visu etatu, ne visu etatu ir pagal sutartį)

2.1.2 išorės paslaugų teikėjus, konsultantus ir tiekėjus

2.1.3 laikinus ir projektinius darbuotojus, kuriems patvirtinta nuotolinė prieiga

**2.2 Politika apima:**

2.2.1 prieigą prie organizacijos sistemų per virtualųjį privatųjį tinklą (VPN) arba patvirtintas nuotolinės prieigos priemones

2.2.2 jautrios ir reglamentuojamos informacijos tvarkymą už saugių patalpų ribų

2.2.3 organizacijai priklausančios įrangos arba nuosavų įrenginių naudojimą (BYOD)

2.2.4 fizines ir logines apsaugos priemones nuotolinėse aplinkose

2.3 Ši politika taikoma visose geografinėse vietovėse ir laiko juostose, kuriose organizacija leidžia nuotolinį darbą, nepriklausomai nuo to, ar jis yra nuolatinis, ad hoc, ar taikomas veiklos tęstinumo įvykių metu.

## 3. Tikslai

3.1 Užtikrinti, kad tik autorizuoti asmenys galėtų nuotoliniu būdu pasiekti vidines sistemas ir informaciją.

3.2 Užtikrinti šifravimo, kelių veiksnių autentifikavimo (MFA) ir galinių įrenginių saugumo priemonių taikymą visuose nuotolinės prieigos kanaluose.

3.3 Palaikyti saugumo būklę, atsparią tokioms grėsmėms kaip fišingas, kenkėjiška programinė įranga, duomenų iškėlimas ir neautorizuotas išorinis sistemų pasiekiamumas.

3.4 Nustatyti jautrių duomenų perdavimo, saugojimo ir spausdinimo ne organizacijos patalpose tvarką.

3.5 Integruoti fizinio saugumo priemones, mažinančias matomumo ir neautorizuoto stebėjimo riziką nuotolinių sesijų metu.

3.6 Užtikrinti atitiktį tarptautiniams reguliavimo reikalavimams, taikomiems nuotolinei prieigai prie duomenų, įskaitant ES BDAR, NIS2 direktyvą ir DORA reglamentą.

## 4. Vaidmenys ir atsakomybės

**4.1 Vykdomoji vadovybė**

4.1.1 Tvirtina šią politiką ir užtikrina, kad būtų skirti reikalingi ištekliai bei kad ji būtų integruota į žmogiškųjų išteklių, IT ir saugumo operacijas.

4.1.2 Tvirtina organizacijos nuotolinio darbo tinkamumo kriterijus ir jų taikymą verslo padaliniuose.

**4.2 Vyriausiasis informacijos saugumo pareigūnas / ISVS vadovas**

4.2.1 Yra šios politikos savininkas, ją prižiūri ir užtikrina jos suderinamumą su rizikos laikysena ir reguliavimo reikalavimais.

4.2.2 Nustato nuotolinės prieigos saugos kontrolės priemones (pvz., šifravimą, galinių įrenginių apsaugą, sesijų laiko limitus).

4.2.3 Tvirtina išimčių valdymą ir stebi kontrolės priemonių veiksmingumą.

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

## 9. Peržiūros ir atnaujinimo reikalavimai

### 9.1 Peržiūros dažnumas

#### 9.1.1 Ši politika turi būti peržiūrima kasmet arba dažniau, kai:

9.1.1.1 įdiegiamos naujos nuotolinės prieigos technologijos

9.1.1.2 reikšmingai išplečiamas nuotolinis darbas (pvz., hibridinės darbo jėgos iniciatyvos)

9.1.1.3 atsiranda naujų grėsmių, pažeidžiamumų arba incidentų, susijusių su nuotolinėmis aplinkomis

9.1.1.4 pasikeičia taikomos teisinės arba reguliavimo sistemos

### 9.2 Savininkystė ir peržiūros procesas

#### 9.2.1 Politikos savininkas yra CISO. Peržiūra turi būti koordinuojama su:

9.2.1.1 IT operacijomis ir architektūra

9.2.1.2 žmogiškaisiais ištekliais ir patalpų bei turto valdymo funkcija (dėl operacinių ir darbo vietos pasekmių)

9.2.1.3 duomenų apsaugos pareigūnu (dėl privatumo ir tarpvalstybinių duomenų kontrolės priemonių)

#### 9.2.2 Politikos atnaujinimai privalo būti:

9.2.2.1 patvirtinti Informacijos saugumo valdymo komiteto

9.2.2.2 komunikuoti visam paveiktam personalui ir rangovams

9.2.2.3 integruoti į įvadinių ir žinių atnaujinimo mokymų medžiagą

### 9.3 Dokumentų kontrolė ir platinimas

9.3.1 Politikoje turi būti nurodytas versijų valdymas, įsigaliojimo data ir versijų istorija.

9.3.2 Pakeistos ankstesnės versijos turi būti saugomos pagal Dokumentų valdymo politiką (P14).

9.3.3 Atnaujintos versijos turi inicijuoti privalomą pakartotinį patvirtinimą naudotojams, kuriems leidžiamas nuotolinis darbas.

## 10. Susijusios politikos ir sąsajos

### 10.1 Ši politika taikoma kartu su:

10.1.1 P1 – Informacijos saugumo politika: nustato bazinius saugaus turto tvarkymo reikalavimus, taikomus visose darbo aplinkose, įskaitant nuotolinę.

10.1.2 P3 – Priimtino naudojimo politika: reglamentuoja tinkamą organizacijos įrenginių ir sistemų naudojimą nuotolinio darbo sesijų metu.

10.1.3 P4 – Prieigos kontrolės politika: užtikrina, kad nuotolinės prieigos teisės būtų suteikiamos pagal mažiausių privilegijų principą ir taikant tinkamus autentifikavimo mechanizmus.

10.1.4 P6 – Rizikos valdymo politika: nustato, kaip nuotolinio darbo rizikos identifikuojamos, tvarkomos ir stebimos ISVS sistemoje.

10.1.5 P12 – Turto valdymo politika: reikalauja visų nuotoliniam darbui naudojamų įrenginių apskaitos ir konfigūracijų valdymo.

10.1.6 P22 – Žurnalų tvarkymo ir stebėsenos politika: užtikrina, kad nuotolinės sesijos būtų stebimos, audituojamos ir saugomos pagal atitikties reikalavimus.

10.1.7 P14 – Duomenų saugojimo ir sunaikinimo politika: nustato nuotoliniam darbui aktualias duomenų tvarkymo taisykles, įskaitant išimamas laikmenas ir įrenginių šalinimą.

10.2 Šios politikos kartu užtikrina, kad nuotolinis darbas būtų saugus, atitiktų reikalavimus ir būtų įgyvendinamas visose funkcijose bei geografinėse vietovėse.

## 11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintomis saugumo, duomenų apsaugos ir IRT rizikos valdymo sistemomis, siekiant užtikrinti saugią, atsekamą ir reikalavimus atitinkančią nuotolinio darbo praktiką.

### 11.2 ISO/IEC 27001

11.2.1 6.1.3 skyrius – Rizikos tvarkymo planavimas: ši politika prisideda prie rizikų, susijusių su nuotoline prieiga ir paskirstytomis darbo aplinkomis, valdymo.

11.2.2 8.1 skyrius – Veiklos planavimas ir kontrolė: reikalauja įgyvendinti kontrolės priemones sistemoms, pasiekiamoms už organizacijos patalpų ribų.

11.2.3 A priedo kontrolė 6.7 – Nuotolinis darbas: ši politika visapusiškai apima reikalaujamas informacijos saugumo kontrolės priemones, kai personalas dirba už organizacijos patalpų ribų, įskaitant fizines ir logines apsaugos priemones, prieigos valdyseną ir naudotojų elgsenos stebėseną.

### 11.3 ISO/IEC 27002:2022 – Kontrolė 6

11.3.1 Ši kontrolė nustato procedūrines ir technines apsaugos priemones nuotoliniam darbui. Ji apima įrenginių saugumo, prieigos metodų, duomenų tvarkymo, aplinkos apsaugos priemonių ir trečiųjų šalių dalyvių valdymo reikalavimus, kurie visi įgyvendinami šia politika.

### 11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Nuotolinė prieiga): tiesiogiai įgyvendinama per VPN kontrolės priemones, MFA, sesijų žurnalus ir vaidmenimis grindžiamą nuotolinių naudotojų prieigos autorizavimą.

11.4.2 AC-2 (Paskyrų valdymas): kontroliuoja prieigos tinkamumą, nuotolinių privilegijų priskyrimą ir paskyrų išjungimą.

11.4.3 SC-12–SC-13 (kriptografinė apsauga, kriptografinių raktų nustatymas): įgyvendinama per privalomą VPN naudojimą ir viso disko šifravimą nuotoliniams galiniams įrenginiams.

11.4.4 MP-5 (laikmenų transportavimo apsauga) ir PE-18 (informacijos sistemos komponentų vieta): nuotolinio darbo gairės nustato transportavimo apsaugą ir fizines apsaugos priemones už organizacijos ribų esančiose aplinkose.

11.4.5 AU-2, AU-6: nuotolinių sesijų žurnalai ir stebėsena palaiko audito ir reagavimo į incidentus reikalavimus.

### 11.5 ES BDAR (2016/679)

11.5.1 32 straipsnis – Tvarkymo saugumas: ši politika nustato nuotolinės prieigos saugumo, šifravimo ir žurnalų vedimo kontrolės priemones, būtinas apsaugoti asmens duomenis, pasiekiamus ar tvarkomus nuotoliniu būdu.

11.5.2 5 straipsnio 1 dalies f punktas: užtikrina, kad už organizacijos ribų pasiekiami asmens duomenys būtų apsaugoti nuo neautorizuoto ar neteisėto tvarkymo ir atsitiktinio praradimo.

11.5.3 39 konstatuojamoji dalis: pabrėžia prieigos ribojimą, vientisumą ir konfidencialumą, ypač kai įrenginiai išnešami iš saugių patalpų.

### 11.6 ES NIS2 direktyva (2022/2555)

11.6.1 21 straipsnio 2 dalies a, b, d punktai: reikalauja, kad nuotolinė prieiga būtų apsaugota kaip organizacijos IRT rizikos valdymo sistemos dalis. Ši politika įgyvendina reikalavimą taikyti saugumo priemones, apimančias prieigos kontrolę, duomenų saugumą ir organizacines politikas nuotolinėms aplinkoms.

11.6.2 21 straipsnio 3 dalis: skatina saugumo suvokimą ir politikos laikymąsi tarp darbuotojų, dirbančių už pagrindinių patalpų ribų.

**11.7 ES DORA reglamentas (2022/2554)**

11.7.1 5 straipsnis – Valdysena ir vidaus kontrolės sistema: ši politika palaiko IRT rizikos kontrolės lūkesčius visuose veiklos scenarijuose, įskaitant hibridinius ir nuotolinius modelius.

11.7.2 8 straipsnis – IRT rizikos valdymo sistema: nuotolinės prieigos rizikos čia identifikuojamos, mažinamos ir valdomos taikant technines ir organizacines kontrolės priemones.

11.7.3 9 straipsnis – Susitarimai dėl dalijimosi informacija: apsaugo nuo nuotolinio informacijos nutekėjimo skaitmeninio operacinio atsparumo tinkluose dalijantis informacija.

**11.8 COBIT 2019**

11.8.1 DSS01 – Valdomos operacijos: ši politika palaiko saugų veiklos tęstinumą nepriklausomai nuo fizinės vietos.

11.8.2 BAI06 – Valdomi IT pakeitimai ir BAI09 – Valdomas turtas: užtikrina, kad nuotolinio darbo įrenginiai būtų sekami, saugiai konfigūruojami ir tvarkomi kaip kritinis turtas.

11.8.3 APO13 – Valdomas saugumas: skatina apibrėžtą saugumo valdysenos sistemą nuotolinėms aplinkoms.

11.8.4 MEA03 – Atitikties stebėsena, vertinimas ir peržiūra: nustato, kad nuotolinio darbo veikla turi būti registruojama, peržiūrima ir audituojama.