| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Čia įrašykite registruoto juridinio asmens pavadinimą | | | | | | | |
| Dokumento numeris:<br>P10 | | | | | Dokumento pavadinimas:<br>**Švaraus stalo ir ekrano 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

Suderinta su standartais ir reglamentais

| Standartas / reglamentas | Punktas / straipsnis | Komentaras |
|---|---|---|
| ISO/IEC 27001:2022 | 6.1.3 punktas, 8 punktas | Rizikos tvarkymo planas, operacinis planavimas ir saugių darbo vietų kontrolė |
| ISO/IEC 27002:2022 | Kontrolė 7 | Elgsenos ir aplinkos kontrolės priemonės, skirtos apsaugoti be priežiūros paliktą fizinę informaciją |
| NIST SP 800-53 Rev.5 | PE-2, PS-7, MP-6, AC-11, CM-6, IA-5 | Fizinė prieiga, išorės personalo saugumas, laikmenų sunaikinimas, sesijos užrakinimas, konfigūracijos ir autentifikavimo priemonių kontrolė |
| ES BDAR | 5 straipsnio 1 dalies f punktas, 32 straipsnis; 39 konstatuojamoji dalis | Duomenų vientisumas, konfidencialumas ir fizinės duomenų apsaugos priemonės |
| ES NIS2 direktyva | 21 straipsnio 2 dalies d punktas, 21 straipsnio 3 dalis | Fizinio saugumo, naudotojų elgsenos ir duomenų nutekėjimo prevencijos politikos |
| ES DORA reglamentas | 5, 8, 9 straipsniai | Vidaus valdymas, IRT ir incidentų valdymas, apimantys fizinį saugumą |
| COBIT 2019 | DSS01, DSS05, MEA | Valdomos operacijos, saugumo paslaugos ir atitikties stebėsena |

**1. Tikslas**

1.1 Ši politika nustato privalomas kontrolės priemones, skirtas apsaugoti jautrią informaciją, reikalaujant saugaus fizinių dokumentų, darbo vietų, ekranų ir keičiamųjų laikmenų tvarkymo biuruose ir bendrose darbo erdvėse.

1.2 Ji įgyvendina ISO/IEC 27001 A priedo 7.7 kontrolę, nustatydama elgsenos ir technines praktikas, mažinančias neteisėto atskleidimo, vagystės ar duomenų praradimo riziką dėl be priežiūros paliktos arba matomos informacijos.

1.3 Ši politika stiprina fizinį ir informacijos saugumą kasdienėje veikloje ir padeda užtikrinti taikomų teisinių, sutartinių ir reguliavimo reikalavimų laikymąsi.

**2. Taikymo sritis**

**2.1 Ši politika taikoma visam personalui, kuris dirba fizinėse darbo erdvėse arba turi prie jų prieigą, įskaitant:**

2.1.1 nuolatinius ir laikinus darbuotojus

2.1.2 rangovus, konsultantus, tiekėjus ir praktikantus

2.1.3 trečiųjų šalių paslaugų teikėjus ir vietoje esančius lankytojus, turinčius prieigą prie jautrios informacijos

**2.2 Reikalavimai taikomi:**

2.2.1 individualiuose kabinetuose, darbo vietų kabinose ir atviro plano darbo erdvėse

2.2.2 posėdžių kambariuose ir bendrose bendradarbiavimo erdvėse

2.2.3 spausdintuvų zonose, registratūrose ir kopijavimo patalpose

2.2.4 vietose, kur naudojamos nuotolinės darbo vietos arba bendri kioskai

2.3 Ši politika taip pat taikoma laikinoms ar hibridinėms darbo aplinkoms (pvz., nuolat nepriskirtoms darbo vietoms) ir viešai matomoms aplinkoms, kuriose kyla stebėjimo per petį ar be priežiūros paliktų duomenų rizika.

**3. Tikslai**

3.1 Užkirsti kelią neteisėtai prieigai prie konfidencialios, jautrios ar reguliuojamos informacijos, paliktos atviroje fizinėje ar skaitmeninėje formoje.

3.2 Skatinti standartizuotą saugumo laikyseną visose darbo aplinkose, taikant fizines apsaugos priemones, darbo vietų konfigūraciją ir galutinių naudotojų elgseną.

3.3 Mažinti privatumo pažeidimų, intelektinės nuosavybės praradimo ir duomenų nutekėjimo riziką, kylančią dėl neatsargumo ar priežiūros stokos.

3.4 Įtvirtinti švaraus stalo ir ekrano praktiką organizacijos kultūroje, stiprinant veiklos drausmę, audituojamumą ir galimybę pagrįsti atitiktį.

3.5 Padėti užtikrinti atitiktį ISO/IEC 27001, ES BDAR 32 straipsnio, NIS2 direktyvos 15 straipsnio ir kitų fizinio saugumo reikalavimų, susijusių su kritiniais ar asmens duomenimis, nuostatoms.

**4. Vaidmenys ir atsakomybės**

**4.1 Vadovybė**

4.1.1 Tvirtina šią politiką ir skatina saugumo suvokimu grindžiamą kultūrą visuose verslo padaliniuose.

4.1.2 Skiria tinkamus išteklius politikos įgyvendinimui, informuotumo didinimo kampanijoms ir fizinės kontrolės priemonėms.

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

4.2.1 Yra šios politikos savininkas ir užtikrina jos suderinamumą su ISO/IEC 27001:2022, audito reikalavimais ir rizikos tvarkymo strategijomis.

4.2.2 Rengia informuotumo didinimo programas ir kontrolės priemones, kad būtų užtikrintas nuoseklus įgyvendinimas visose patalpose ir hibridinėse darbo aplinkose.

4.2.3 Koordinuoja veiksmus su patalpų ir turto valdymo bei IT funkcijomis, kad būtų įdiegtos tinkamos fizinės apsaugos priemonės.

[ ... 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 tvarkaraštis**

**9.1.1 Ši politika turi būti peržiūrima:**

9.1.1.1 ne rečiau kaip kartą per metus

9.1.1.2 po bet kokios su darbo vietos ar ekrano atvirumu susijusios audito neatitikties

9.1.1.3 po fizinio ar aplinkos incidento (pvz., įrenginio vagystės, patekimo iš paskos, stebėjimo)

9.1.1.4 įdiegus naujus biuro išdėstymus, patalpų politikas ar darbo vietų modelius (pvz., laikinąsias darbo vietas, nuotolinius centrus)

**9.2 Atsakingi savininkai**

9.2.1 Politikos savininkas yra vyriausiasis informacijos saugumo pareigūnas arba paskirtas ISVS vadovas.

**9.2.2 Peržiūros procese turi dalyvauti:**

9.2.2.1 patalpų ir organizacijos saugumo komandos

9.2.2.2 IT ir infrastruktūros funkcijos dėl su įrenginiais susijusio taikymo užtikrinimo

9.2.2.3 žmogiškųjų išteklių ir teisės funkcijos dėl elgsenos reikalavimų taikymo ir suderinimo su drausminėmis priemonėmis

9.2.3 Visi politikos atnaujinimai turi būti valdomi taikant versijų kontrolę, patvirtinami ISVS valdymo komiteto ir, prireikus, pakartotinai išplatinami su nauju patvirtinimu.

**9.3 Pakeitimų komunikavimas**

**9.3.1 Naudotojai turi būti informuojami apie esminius atnaujinimus per:**

9.3.1.1 intraneto politikų centrą arba portalą

9.3.1.2 tikslinius el. pašto pranešimus

9.3.1.3 pakartotinius įvedimo į darbą mokymus ir ketvirtinius instruktažus

9.3.1.4 privalomus patvirtinimo pranešimus dėl bet kokių naujų kritinių įgyvendinimo nuostatų

**10. Susijusios politikos ir sąsajos**

**10.1 Ši politika yra suderinta su šiomis politikomis ir jas papildo:**

10.1.1 P1 – Informacijos saugumo politika: nustato naudotojų elgsenos ir fizinio saugumo lūkesčius, kurie yra šios politikos pagrindas.

10.1.2 P3 – Priimtino naudojimo politika: apibrėžia naudotojų atskaitomybę už duomenų ir sistemų apsaugą, įskaitant fizines aplinkas.

10.1.3 P6 – Rizikos valdymo politika: įtraukia fizinių darbo erdvių rizikas į visos organizacijos informacijos rizikos analizę.

10.1.4 P12 – Turto valdymo politika: padeda užtikrinti ant stalų paliekamų įrenginių ir laikmenų apskaitą bei saugų tvarkymą.

10.1.5 P13 – Duomenų klasifikavimo ir ženklinimo politika: susieja švaraus stalo kontrolę su fiziniais dokumentais, pažymėtais kaip konfidencialūs arba skirti vidaus naudojimui.

10.1.6 P14 – Duomenų saugojimo terminų ir sunaikinimo politika: nustato fizinių dokumentų saugojimo, naikinimo ir talpų naudojimo praktikas.

10.1.7 P22 – Žurnalų tvarkymo ir stebėsenos politika: gali būti naudojama darbo vietų užrakinimo būsenai, neaktyvumo laikui ar darbo vietų kamerų srautams stebėti, kai tai leidžiama.

10.2 Šios susijusios politikos kuria integruotą saugumo kultūrą, derindamos naudotojų informuotumą, fizines apsaugos priemones ir atskaitomybę, kad būtų užtikrintos atsparios darbo erdvės.

**11. Pamatiniai standartai ir sistemos**

11.1 Ši politika yra suderinta su visuotinai pripažintais standartais ir teisiniais reikalavimais, nustatančiais pareigą saugoti jautrią informaciją fizinėse aplinkose ir valdant naudotojų elgseną.

**11.2 ISO/IEC 27001**

11.2.1 6.1.3 punktas – Rizikos tvarkymo planas: padeda įgyvendinti kontrolės priemones, skirtas fizinei ir aplinkos rizikai mažinti, įskaitant riziką, susijusią su naudotojų elgsena atvirose darbo erdvėse.

11.2.2 8.1 punktas – Operacinis planavimas ir kontrolė: nustato operacines apsaugos priemones saugių darbo vietų ir įrangos naudojimo valdymui.

**11.3 ISO/IEC 27002:2022 – Kontrolė 7**

11.3.1 Ši kontrolė reikalauja elgsenos ir aplinkos apsaugos priemonių, kurios užkirstų kelią neteisėtai prieigai prie informacijos per be priežiūros paliktas laikmenas, ekranus ar atspausdintą medžiagą. Ši politika nustato fizinių darbo erdvių tvarkos palaikymą, ekrano užrakinimo naudojimą ir jautrių dokumentų sunaikinimą.

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

11.4.1 PE-2 (Physical Access Authorizations): siejama su darbo vietų apribojimais ir rakinamo saugojimo reikalavimų taikymu aukštos rizikos aplinkose.

11.4.2 PS-7 (External Personnel Security): taikoma per švaraus stalo ir ekrano reikalavimus, išplėstus rangovams ir trečiųjų šalių naudotojams.

11.4.3 MP-6 (Media Sanitization) ir AC-11 (Session Lock): įgyvendinamos per saugaus sunaikinimo procedūras ir privalomus ekrano užrakinimo laikmačius.

11.4.4 CM-6 (Configuration Settings) ir IA-5 (Authenticator Management): palaiko techninį ekrano užrakinimo ir sesijos kontrolės taikymą galiniuose įrenginiuose.

**11.5 ES BDAR (2016/679)**

11.5.1 5 straipsnio 1 dalies f punktas: nustato asmens duomenų vientisumo ir konfidencialumo užtikrinimą, įskaitant apsaugą nuo fizinio atvirumo ar peržiūros neįgaliotiems asmenims.

11.5.2 32 straipsnis – Tvarkymo saugumas: reikalauja tinkamų fizinių ir organizacinių priemonių asmens duomenims apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, praradimo ar neteisėto atskleidimo – tai įgyvendinama taikant stalo ir ekrano kontrolės priemones.

11.5.3 39 konstatuojamoji dalis: reikalauja riboti prieigą prie asmens duomenų tik įgaliotiems asmenims – tai apima ir jų apsaugą fizine forma, kai jie paliekami be priežiūros.

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

11.6.1 21 straipsnio 2 dalies d punktas: reikalauja politikų ir procedūrų, susijusių su fiziniu ir aplinkos saugumu, įskaitant darbo vietos lygmens informacijos saugumo apsaugos priemones.

11.6.2 21 straipsnio 3 dalis: skatina saugumo kultūrą, apimančią tinkamą naudotojų elgseną, informuotumą ir netyčinio duomenų nutekėjimo prevenciją – tai palaikoma šios politikos elgsenos kontrolės priemonėmis.

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

11.7.1 5 straipsnis – Vidaus valdymas ir kontrolė: reikalauja, kad visos su IRT susijusios rizikos, įskaitant žmogiškąsias ir aplinkos grėsmes, būtų valdomos įgyvendinamomis politikomis.

11.7.2 8 straipsnis – IRT rizikos valdymas: nustato apsaugos priemones tiek skaitmeniniame, tiek fiziniame kontekste, užtikrinant, kad nuotoliniai, filialų ir vietinės infrastruktūros naudotojai nesukurtų nevaldomo išorinio pasiekiamumo.

11.7.3 9 straipsnis – Incidentų valdymas: reikalauja, kad aplinkos ar elgsenos trūkumai, lemiantys duomenų atvirumą, būtų registruojami, klasifikuojami ir tvarkomi taikant tinkamus korekcinius veiksmus.

**11.8 COBIT 2019**

11.8.1 DSS01 – Managed Operations: užtikrina operacinę drausmę saugant fizines darbo erdves ir sistemas per pakartojamas kontrolės priemones.

11.8.2 DSS05 – Managed Security Services: palaiko duomenų, įrenginių ir prieigos galinių taškų apsaugą taikant elgsena grindžiamas priemones, tokias kaip švaraus stalo praktika.

11.8.3 MEA03 – Monitor, Evaluate, and Assess Compliance: skatina fizinių apsaugos priemonių ir politikos taikymo auditavimą kasdienėje veikloje.