					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P10S					Dokumento pavadinimas: **Švaraus darbo stalo ir ekrano 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	7.2, 8 skyriai	
ISO/IEC 27002:2022	Kontrolė 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	
ES DORA reglamentas	9 straipsnio 2 dalies f punktas	
COBIT 2019	DSS01.06, DSS05	
ES BDAR	32 straipsnis	

1. Tikslas

1.1 Ši politika nustato privalomuosius reikalavimus saugiai darbo aplinkai palaikyti, užtikrinant, kad darbo stalai, darbo vietos ir ekranai, palikti be priežiūros, nebūtų su matoma konfidencialia informacija.

1.2 Pagrindinis šios politikos tikslas – užkirsti kelią neteisėtai prieigai prie jautrios informacijos dėl be priežiūros paliktų spausdintų dokumentų, neužrakintų ekranų ar netinkamai paliktų keičiamųjų laikmenų tiek biuro patalpose, tiek nuotolinio darbo vietose.

1.3 Šioje politikoje apibrėžta švaraus darbo stalo ir ekrano praktika stiprina organizacijos gebėjimą atitikti ISO/IEC 27001 sertifikavimo reikalavimus, mažindama išvengiamo informacijos atskleidimo riziką. Ši praktika taip pat suteikia klientams, partneriams ir auditoriams užtikrintumą, kad informacijos saugumas organizacijoje yra vertinamas rimtai net ir ribotų išteklių sąlygomis.

1.4 Ši politika palaiko atskaitomybės ir saugumo suvokimo kultūrą, užtikrindama, kad visas personalas, nepriklausomai nuo pareigų ar techninės kompetencijos, suprastų savo atsakomybę apsaugoti organizacijos ir klientų informaciją nuo vizualinio atskleidimo, vagystės ar praradimo.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems darbuotojams, rangovams, praktikantams ir laikiniesiems darbuotojams, naudojantiems organizacijai priklausančias arba jiems priskirtas darbo vietas, darbo stalus ar mobiliuosius įrenginius

2.1.2 Visoms fizinėms vietoms, naudojamoms veiklai vykdyti, įskaitant skirtus biurus, bendradarbystės erdves ir nuotolinio darbo / namų darbo vietas

2.1.3 Visiems skaitmeniniams įrenginiams su ekranais, įskaitant stalinius kompiuterius, nešiojamuosius kompiuterius, planšetes ir išorinius monitorius, naudojamus veiklos tikslais

2.2 Politika taip pat taikoma bet kokiam fiziniam ar skaitmeniniam turtui, kuris gali rodyti, saugoti ar perduoti jautrią informaciją, įskaitant:

2.2.1 Spausdintus dokumentus ar ranka rašytas pastabas

2.2.2 USB laikmenas, CD diskus ir išorinius standžiuosius diskus

2.2.3 Mobiliuosius telefonus, naudojamus verslo pranešimams ar el. paštui

2.2.4 Kompiuterių monitorius ir projektorius, prijungtus prie darbo sistemų

2.3 Ši politika galioja ir ne įprastomis darbo valandomis bei nestandartinių operacijų metu (pvz., atliekant priežiūros darbus po darbo valandų arba vykdant skubaus reagavimo darbus).

3. Tikslai

3.1 Įgyvendinti praktiškas ir nuoseklias kontrolės priemones, užtikrinančias, kad ant darbo stalų, ekranuose ar bendrose erdvėse neliktų atvirai matomos jautrios informacijos.

3.2 Sumažinti neteisėtos prieigos riziką tiek iš vidinių šaltinių (pvz., kitų darbuotojų netyčinė prieiga), tiek dėl išorinių grėsmių (pvz., lankytojų, valymo personalo ar rangovų).

3.3 Palaikyti loginės ir fizinės prieigos valdymą, nustatant darbuotojams pareigą aktyviai apsaugoti darbo medžiagą ir užrakinti kompiuterius paliekant darbo vietą be priežiūros.

3.4 Didinti darbuotojų informuotumą apie saugaus darbo praktiką ir nustatyti paprastas, privalomas taisykles, taikomas kasdienėje veikloje, nepriklausomai nuo darbo vietos.

3.5 Užtikrinti atitiktį ISO/IEC 27001 A priedo 7.7 kontrolei ir jos įgyvendinimo gairėms pagal ISO/IEC 27002 dėl švaraus darbo stalo ir ekrano reikalavimų.

3.6 Užtikrinti, kad organizacija galėtų pademonstruoti deramą rūpestingumą ir pasirengimą auditui, nereikalaujant didelės apimties įmonės infrastruktūros.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 Yra šios politikos savininkas ir užtikrina, kad ji būtų tinkamai komunikuojama, suprantama ir kad jos laikytųsi visi darbuotojai bei rangovai.

4.1.2 Atsako už visų išimčių tvirtinimą, reagavimą į pažeidimus ir saugaus darbo praktikos mokymų priežiūrą.

4.1.3 Privalo vykdyti arba pavesti vykdyti reguliarius patikrinimus (ne rečiau kaip kartą per ketvirtį), kad patvirtintų, jog fizinės ir skaitmeninės darbo vietos atitinka politikos reikalavimus.

4.2 Paskirtas darbuotojas (jei paskirtas)

4.2.1 Gali būti paskirtas atsakingu už techninių konfigūracijų įgyvendinimą (pvz., ekrano užrakinimo po neveiklos nustatymus) arba fizinių saugojimo priemonių (pvz., rakinamų stalčių) paskirstymą.

4.2.2 Padeda GM, pranešdamas apie neatitiktis, teikdamas priminimus dėl darbo vietos saugumo ir stebėdamas korekcinių veiksmų įgyvendinimą nustačius trūkumus.

4.2.3 Padeda užtikrinti, kad visi darbuotojai, kai tai įmanoma, turėtų prieigą prie tinkamų rakinimo priemonių arba saugių saugojimo vietų.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 GM privalo peržiūrėti šią politiką bent kartą per metus ir po bet kurio iš šių įvykių:

9.1.1 Naujų biuro erdvių, įrenginių ar bendro naudojimo sistemų įdiegimo

9.1.2 Taikomų teisinių ar sertifikavimo reikalavimų pasikeitimo

9.1.3 Audito išvadų, rizikos vertinimų ar saugumo incidentų

9.2 Tarpiniai atnaujinimai turi būti komunikuojami visiems darbuotojams el. paštu, reikalaujant patvirtinimo.

9.3 Ankstesnės šios politikos versijos turi būti saugomos saugiai ir būti prieinamos auditui, kad parodytų nuolatinę atitiktį ISO/IEC 27001 ir susijusioms sistemoms.

10. Susijusios politikos ir sąsajos

10.1 P2S – Valdysenos vaidmenų ir atsakomybių politika: paaiškina GM įgaliojimus užtikrinti fizinės ir skaitmeninės darbo vietos elgsenos reikalavimų laikymąsi ir atlikti jų auditą.

10.2 P4S – Prieigos kontrolės politika: palaiko techninį ekrano užrakinimo ir saugaus prisijungimo prie darbo vietos praktikos įgyvendinimą.

10.3 P8S – Informacijos saugumo supratimo ir mokymo politika: sustiprina elgsenos mokymus, reikalingus šios politikos laikymuisi.

10.4 P17S – Duomenų apsaugos ir privatumo politika: apibrėžia pareigas tvarkant ir saugant asmens duomenis bei kitus jautrius duomenis laikantis BDAR reikalavimų.

10.5 P30S – Reagavimo į incidentus politika: nustato eskalavimo ir reagavimo tvarką, kai dėl pažeidimo įvyksta duomenų atskleidimas arba duomenų saugumo pažeidimas.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 7.2 skyrius: reikalauja, kad visas personalas žinotų saugumo atsakomybes, įskaitant fizines apsaugos priemones.

11.1.2 8.1 skyrius: operacinės kontrolės priemonės turi užtikrinti tinkamas logines ir fizines apsaugos priemones.

11.2 ISO/IEC 27002

11.2.1 Kontrolė 7.7: pateikia išsamias gaires dėl švaraus darbo stalo ir ekrano reikalavimų nustatymo, komunikavimo ir taikymo.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: nustato fizinės prieigos kontrolės lūkesčius, įskaitant personalo elgesį saugiose aplinkose.

11.3.2 AC-11: nustato privalomą sesijos užrakinimo funkcionalumą darbo vietoms, kad būtų išvengta neteisėto peržiūrėjimo ar sąveikos.

11.4 ES BDAR

11.4.1 32 straipsnis: reikalauja, kad organizacijos saugotų asmens duomenis taikydamos fizines ir technines apsaugos priemones, įskaitant darbo vietas ir dokumentus.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies d punktas: reikalauja, kad organizacijos įgyvendintų rizika grindžiamas fizinės ir loginės prieigos politikas.

11.6 ES DORA reglamentas

11.6.1 9 straipsnio 2 dalies f punktas: nustato IRT saugumo politikų reikalavimą, įskaitant saugią darbo vietos higieną, finansų sektoriaus subjektams ir jų tiekimo grandinėms.

11.7 COBIT 2019

11.7.1 DSS01.06: reikalauja turto apsaugos praktikos, įskaitant fizines darbo vietų ir laikmenų kontrolės priemones.

11.7.2 DSS05.02: palaiko galutinių naudotojų saugumo praktikos taikymą visose veiklos aplinkose.