					Šeit ievadiet reģistrētās juridiskās personas nosaukumu						
Dokumenta numurs: P10S					Dokumenta nosaukums: **tīrā galda un ekrāna politika**						
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:						
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	7.2., 8. punkts	
ISO/IEC 27002:2022	7. kontrole	
NIST SP 800-53 Rev.5	PE-2, AC-11	
ES NIS2	21. panta 2. punkta d) apakšpunkts	
ES DORA	9. panta 2. punkta f) apakšpunkts	
COBIT 2019	DSS01.06, DSS05	
ES VDAR	32. pants	

1. Mērķis

1.1 Šī politika nosaka saistošas prasības drošas darba vides uzturēšanai, nodrošinot, ka bez uzraudzības atstātos galdos, darbvietās un displeju ekrānos nav redzama konfidenciāla informācija.

1.2 Tās galvenais mērķis ir novērst nesankcionētu piekļuvi sensitīvai informācijai, ko var izraisīt bez uzraudzības atstāti izdrukāti dokumenti, nebloķēti ekrāni vai neatbilstoši novietoti noņemamie datu nesēji gan fiziskajās biroja telpās, gan attālinātā darba vietās.

1.3 Šajā politikā noteiktā tīrā galda un ekrāna prakse stiprina organizācijas spēju izpildīt ISO/IEC 27001 sertifikācijas prasības, samazinot novēršamus pakļautības riskus. Tā arī apliecina klientiem, partneriem un auditoriem, ka informācijas drošība tiek uztverta nopietni arī vidēs ar ierobežotiem resursiem.

1.4 Šī politika atbalsta pārskatatbildības un informētības kultūru, nodrošinot, ka viss personāls neatkarīgi no amata vai tehniskās kompetences izprot savu pienākumu aizsargāt uzņēmuma un klientu informāciju pret vizuālu atklāšanu, zādzību vai zaudējumu.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem darbiniekiem, līgumslēdzējiem, praktikantiem un pagaidu darbiniekiem, kuri izmanto uzņēmumam piederošas vai personiski piešķirtas darbvietas, galdus vai mobilās ierīces;

2.1.2 visām fiziskajām vietām, kas tiek izmantotas uzņēmējdarbībai, tostarp atsevišķiem birojiem, kopstrādes telpām un attālinātā darba vai mājas darba vietām;

2.1.3 visām digitālajām ierīcēm ar attēlošanas iespējām, tostarp stacionārajiem datoriem, klēpjdatoriem, planšetdatoriem un ārējiem monitoriem, kas tiek izmantoti darba vajadzībām.

2.2 Politika attiecas arī uz jebkuru fizisku vai digitālu aktīvu, kurā var attēlot, glabāt vai pārsūtīt sensitīvu informāciju, tostarp:

2.2.1 drukātiem ierakstiem vai ar roku rakstītām piezīmēm;

2.2.2 USB datu nesējiem, CD un ārējiem cietajiem diskiem;

2.2.3 mobilajiem tālruņiem, kas tiek izmantoti darba saziņai vai e-pastam;

2.2.4 datoru monitoriem un projektoriem, kas ir pieslēgti darba sistēmām.

2.3 Šī politika ir piemērojama arī ārpus noteiktā darba laika un nestandarta darbību laikā (piemēram, pēc darba laika veikta apkope vai ārkārtas reaģēšanas darbi).

3. Mērķi

3.1 Ieviest praktiskus un konsekventus kontroles pasākumus, kas nodrošina, ka uz galdiem, ekrāniem vai koplietošanas telpās netiek atstāta atklāta sensitīva informācija.

3.2 Samazināt nesankcionētas piekļuves risku gan no iekšējiem avotiem (piemēram, cita darbinieka netīša piekļuve), gan no ārējiem apdraudējumiem (piemēram, apmeklētāji, uzkopšanas personāls vai līgumslēdzēji).

3.3 Atbalstīt loģiskās un fiziskās piekļuves pārvaldības ierobežojumus, nosakot personālam pienākumu aktīvi aizsargāt darba materiālus un bloķēt datorus, kad tie tiek atstāti bez uzraudzības.

3.4 Veicināt personāla izpratni par drošām darba praksēm un noteikt vienkāršas, saistošas prasības, kas piemērojamas ikdienas darbībā neatkarīgi no darba vietas.

3.5 Nodrošināt atbilstību ISO/IEC 27001 A pielikuma 7.7. kontrolei un tās ieviešanas vadlīnijām saskaņā ar ISO/IEC 27002 attiecībā uz tīrā galda un ekrāna prasībām.

3.6 Nodrošināt, ka organizācija var pierādīt pienācīgu rūpību un gatavību auditam, neieviešot uzņēmuma līmeņa infrastruktūru.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 ir šīs politikas īpašnieks un nodrošina, ka tā tiek pienācīgi izziņota, izprasta un ievērota visiem darbiniekiem un līgumslēdzējiem;

4.1.2 ir atbildīgs par jebkuru izņēmumu apstiprināšanu, reaģēšanu uz pārkāpumiem un drošu darba prakšu apmācību uzraudzību;

4.1.3 veic vai deleģē regulāras pārbaudes (vismaz reizi ceturksnī), lai apstiprinātu, ka fiziskās un digitālās darbvietas atbilst šīs politikas prasībām.

4.2 Norīkotais darbinieks (ja iecelts)

4.2.1 var tikt noteikts par atbildīgo par tehnisko konfigurāciju ieviešanu (piemēram, ekrāna automātiskās bloķēšanas iestatījumiem) vai fizisko glabāšanas līdzekļu izsniegšanu (piemēram, aizslēdzamām atvilktnēm);

4.2.2 atbalsta GM, ziņojot par neatbilstībām, sniedzot atgādinājumus par darbvietas drošību un sekojot trūkumu novēršanas pasākumiem, kad tiek konstatētas problēmas;

4.2.3 palīdz nodrošināt, ka visiem darbiniekiem ir pieejami piemēroti bloķēšanas mehānismi vai drošas glabāšanas vietas, ciktāl tas ir iespējams.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 GM pārskata šo politiku vismaz reizi gadā un pēc jebkura no turpmāk minētajiem notikumiem:

9.1.1 jaunu biroja telpu, ierīču vai koplietojamu sistēmu ieviešanas;

9.1.2 izmaiņām piemērojamajās tiesiskajās vai sertifikācijas prasībās;

9.1.3 auditu, risku izvērtējumu vai drošības incidentu secinājumiem.

9.2 Starpposma atjauninājumi ir jāpaziņo visiem darbiniekiem pa e-pastu, pieprasot apliecinājumu.

9.3 Šīs politikas iepriekšējās versijas ir droši jāglabā un jānodrošina to auditējamība, lai apliecinātu nepārtrauktu atbilstību ISO/IEC 27001 un saistītajiem ietvariem.

10. Saistītās politikas un sasaiste

10.1 P2S – Pārvaldības lomu un atbildības politika: precizē GM pilnvaras piemērot šo politiku un veikt fizisko un digitālo darbvietu uzvedības auditu.

10.2 P4S – Piekļuves kontroles politika: atbalsta ekrāna bloķēšanas un drošas pieteikšanās darbvietās tehnisko ieviešanu.

10.3 P8S – Informācijas drošības informētības un apmācību politika: nostiprina uzvedības apmācību, kas nepieciešama atbilstībai šai politikai.

10.4 P17S – Datu aizsardzības un privātuma politika: nosaka pienākumus personas datu un sensitīvu datu apstrādē un aizsardzībā atbilstoši VDAR.

10.5 P30S – Incidentu reaģēšanas politika: nosaka eskalācijas un reaģēšanas ietvaru, ja pārkāpuma rezultātā notikusi datu atklāšana vai personas datu aizsardzības pārkāpums.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 7.2. punkts: nosaka, ka visam personālam ir jāapzinās drošības pienākumi, tostarp fiziskie drošības pasākumi.

11.1.2 8.1. punkts: darbības kontroles pasākumi nodrošina piemērotu fizisko un loģisko aizsardzību.

11.2 ISO/IEC 27002

11.2.1 7.7. kontrole: sniedz detalizētas vadlīnijas tīrā galda un ekrāna prasību noteikšanai, izziņošanai un ieviešanai.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: nosaka fiziskās piekļuves kontroles prasības, tostarp personāla uzvedību aizsargājamās telpās.

11.3.2 AC-11: nosaka pienākumu nodrošināt sesijas bloķēšanas funkcionalitāti darbvietām, lai novērstu nesankcionētu apskati vai mijiedarbību.

11.4 ES VDAR

11.4.1 32. pants: nosaka organizācijām pienākumu aizsargāt personas datus, izmantojot fiziskos un tehniskos kontroles pasākumus, tostarp darbvietu un dokumentu aizsardzību.

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta d) apakšpunkts: nosaka organizācijām pienākumu ieviest uz risku balstītas fiziskās un loģiskās piekļuves politikas.

11.6 ES DORA

11.6.1 9. panta 2. punkta f) apakšpunkts: nosaka IKT drošības politiku nepieciešamību, tostarp drošas darbvietas higiēnu, finanšu sektora dalībniekiem un to piegādes ķēdēm.

11.7 COBIT 2019

11.7.1 DSS01.06: nosaka aktīvu aizsardzības prakses, tostarp fiziskos kontroles pasākumus attiecībā uz darbvietām un datu nesējiem.

11.7.2 DSS05.02: atbalsta gala lietotāju drošības prakšu ievērošanu dažādās darbības vidēs.