					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P10					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 piemērojamajiem standartiem un normatīvajām prasībām

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkts 6.1.3, punkts 8	Risku apstrādes plāns, darbību plānošana un kontrole drošu darbvietu nodrošināšanai
ISO/IEC 27002:2022	7. kontrole	Uzvedības un vides kontroles pasākumi bez uzraudzības atstātas fiziskas informācijas aizsardzībai
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Fiziskā piekļuve, ārējā personāla drošība, datu nesēju likvidēšana, sesijas bloķēšana, konfigurācijas un autentifikācijas kontroles pasākumi
ES VDAR	Panti 5(1)(f), 32; apsvērums 39	Datu integritāte, konfidencialitāte un fiziskie datu aizsardzības pasākumi
ES NIS2	Panti 21(2)(d), 21(3)	Fiziskās drošības, lietotāju uzvedības un datu noplūdes novēršanas politikas
ES DORA	Panti 5, 8, 9	Iekšējā pārvaldība, IKT risku pārvaldība un incidentu pārvaldība saistībā ar fizisko drošību
COBIT 2019	DSS01, DSS05, MEA	Pārvaldītas operācijas, drošības pakalpojumi un atbilstības uzraudzība

1. Mērķis

1.1 Šī politika nosaka obligātus kontroles pasākumus sensitīvas informācijas aizsardzībai, paredzot drošu fizisko dokumentu, darbstaciju, ekrānu un noņemamo datu nesēju apstrādi birojos un koplietojamās darbvietās.

1.2 Tā atbalsta ISO/IEC 27001 A pielikuma 7.7. kontroli, ieviešot uzvedības un tehniskās prakses, kas mazina neatļautas izpaušanas, zādzības vai datu zuduma risku bez uzraudzības atstātas vai redzamas informācijas dēļ.

1.3 Šī politika stiprina fizisko un informācijas drošību ikdienas darbībās un atbalsta atbilstību piemērojamajām tiesiskajām, līgumiskajām un regulatīvajām prasībām.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visu personālu, kas strādā fiziskās darbvietās vai tām piekļūst, tostarp:

2.1.1 Pastāvīgajiem un pagaidu darbiniekiem

2.1.2 Līgumdarbiniekiem, konsultantiem, piegādātājiem un praktikantiem

2.1.3 Trešo pušu pakalpojumu sniedzējiem un apmeklētājiem uz vietas, kuriem ir piekļuve sensitīvai informācijai

2.2 Prasības piemēro šādās vietās:

2.2.1 Individuālos kabinetos, nodalītās darba vietās un atvērtā tipa darbvietās

2.2.2 Sanāksmju telpās un koplietojamās sadarbības zonās

2.2.3 Printeru zonās, reģistratūrās un kopēšanas telpās

2.2.4 Vietās, kur tiek izmantotas attālās darbvirsmas vai koplietojami kioski

2.3 Šī politika attiecas arī uz pagaidu vai hibrīdām darba vidēm (piemēram, hot-desking) un publiski pieejamām vidēm, kur pastāv ekrāna nolasīšanas no malas vai bez uzraudzības atstātas informācijas risks.

3. Mērķi

3.1 Novērst neatļautu piekļuvi konfidenciālai, sensitīvai vai regulētai informācijai, kas fiziskā vai digitālā formā atstāta bez aizsardzības.

3.2 Veicināt standartizētu drošības līmeni visās darba vidēs, izmantojot fiziskos aizsardzības pasākumus, darbstaciju konfigurāciju un galalietotāju uzvedību.

3.3 Samazināt privātuma pārkāpumu, intelektuālā īpašuma neatļautas izpaušanas un datu noplūdes risku, ko rada nolaidība vai nepietiekama uzraudzība.

3.4 Iekļaut tīrā galda un tīra ekrāna paradumus organizācijas kultūrā, atbalstot darbības disciplīnu, auditējamību un tiesisko aizsargātību.

3.5 Atbalstīt atbilstību ISO/IEC 27001, VDAR 32. pantam, NIS2 15. pantam un citām fiziskās drošības prasībām, kas attiecas uz kritiskiem vai personas datiem.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina šo politiku un veicina drošības izpratni visās uzņēmuma struktūrvienībās.

4.1.2 Piešķir atbilstošus resursus politikas ieviešanai, informētības kampaņām un fiziskajiem kontroles pasākumiem.

4.2 Galvenais informācijas drošības vadītājs / IDPS vadītājs

4.2.1 Atbild par šo politiku un nodrošina tās atbilstību ISO/IEC 27001:2022, audita prasībām un risku apstrādes stratēģijām.

4.2.2 Izstrādā informētības programmas un kontroles pasākumus, lai nodrošinātu vienotu ieviešanu visos objektos un hibrīdā darba vidēs.

4.2.3 Sadarbojas ar objektu pārvaldības, aktīvu pārvaldības un IT komandām, lai nodrošinātu atbilstošu fizisko aizsardzības pasākumu ieviešanu.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Politikas pārskatīšanas grafiks

9.1.1 Šī politika jāpārskata:

9.1.1.1 Vismaz reizi gadā

9.1.1.2 Pēc jebkuras ar darbvietas vai ekrāna pakļaušanu riskam saistītas audita neatbilstības

9.1.1.3 Pēc fiziska vai vides incidenta (piemēram, ierīces zādzība, tailgating, novērošana)

9.1.1.4 Pēc jauna biroja plānojuma, objektu politiku vai darbvietu modeļu ieviešanas (piemēram, hot desking, attālinātie darba centri)

9.2 Atbildīgie īpašnieki

9.2.1 Politikas īpašnieks ir Galvenais informācijas drošības vadītājs vai norīkotais IDPS vadītājs.

9.2.2 Pārskatīšanas procesā jāiesaista:

9.2.2.1 Objektu pārvaldības un uzņēmuma drošības komandas

9.2.2.2 IT un infrastruktūras funkcija ar ierīcēm saistītajai politikas piemērošanai

9.2.2.3 Cilvēkresursu (HR) funkcija un Juridiskā un atbilstības funkcija uzvedības prasību piemērošanai un disciplinārās kārtības saskaņošanai

9.2.3 Visi politikas atjauninājumi jāpārvalda ar versiju kontroli, jāapstiprina Informācijas drošības vadības komitejai un, ja nepieciešams, jāizplata atkārtotai apliecināšanai.

9.3 Izmaiņu komunikācija

9.3.1 Lietotāji jāinformē par būtiskiem atjauninājumiem, izmantojot:

9.3.1.1 Intraneta politiku centru vai portālu

9.3.1.2 Mērķētu e-pasta saziņu

9.3.1.3 Ievadapmācības atkārtotos atgādinājumus un ceturkšņa instruktāžas

9.3.1.4 Obligātus apliecinājuma paziņojumus par jebkuriem jauniem kritiskiem politikas piemērošanas punktiem

10. Saistītās politikas un sasaiste

10.1 Šī politika ir saskaņota ar turpmāk norādītajām politikām un tās atbalsta:

10.1.1 P1 – Informācijas drošības politika: nosaka lietotāju uzvedības un fiziskās drošības prasības, kas ir šīs politikas pamats.

10.1.2 P3 – Pieņemamas lietošanas politika: nosaka lietotāju pārskatatbildību par datu un sistēmu aizsardzību, tostarp fiziskajā vidē.

10.1.3 P6 – Risku pārvaldības politika: iekļauj fizisko darbvietu riskus uzņēmuma mēroga informācijas risku analīzē.

10.1.4 P12 – Aktīvu pārvaldības politika: atbalsta uz galdiem atstāto ierīču un datu nesēju uzskaiti un drošu apstrādi.

10.1.5 P13 – Datu klasifikācijas un marķēšanas politika: sasaista tīrā galda prasību ievērošanu ar fiziskiem dokumentiem, kas marķēti kā konfidenciāli vai iekšējai lietošanai.

10.1.6 P14 – Datu glabāšanas un likvidēšanas politika: nosaka fizisko dokumentu glabāšanas, smalcināšanas un tvertņu apstrādes praksi.

10.1.7 P22 – Žurnālfiksēšanas un uzraudzības politika: atļautos gadījumos var tikt izmantota darbstaciju bloķēšanas statusa, dīkstāves laika vai darbvietu kameru plūsmu uzraudzībai.

10.2 Šīs saistītās politikas veido integrētu drošības kultūru, apvienojot lietotāju informētību, fiziskos aizsardzības pasākumus un pārskatatbildību, lai nodrošinātu noturīgas darbvietas.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem standartiem un tiesiskajām prasībām, kas nosaka sensitīvas informācijas aizsardzību fiziskajā vidē un ar lietotāju uzvedību saistītus kontroles pasākumus.

11.2 ISO/IEC 27001

11.2.1 Punkts 6.1.3 – Risku apstrādes plāns: atbalsta kontroles pasākumu ieviešanu fizisko un vides risku mazināšanai, tostarp risku, kas saistīti ar lietotāju uzvedību atvērtās darbvietās.

11.2.2 Punkts 8.1 – Darbību plānošana un kontrole: nosaka darbības aizsardzības pasākumus drošu darbvietu un aprīkojuma lietošanas pārvaldībai.

11.3 ISO/IEC 27002:2022 – 7. kontrole

11.3.1 Šī kontrole nosaka uzvedības un vides aizsardzības pasākumus, lai novērstu neatļautu piekļuvi informācijai caur bez uzraudzības atstātiem datu nesējiem, ekrāniem vai drukātiem materiāliem. Šī politika ievieš fizisko darbvietu higiēnas prasības, ekrāna bloķēšanu un sensitīvu dokumentu likvidēšanu.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Fiziskās piekļuves autorizācijas): saistīts ar darbvietu ierobežojumiem un slēdzamas glabāšanas prasību piemērošanu augsta riska vidēs.

11.4.2 PS-7 (Ārējā personāla drošība): piemērojams, paplašinot tīrā galda un ekrāna prasības uz līgumdarbiniekiem un trešo pušu lietotājiem.

11.4.3 MP-6 (Datu nesēju sanitizācija) un AC-11 (Sesijas bloķēšana): īstenoti ar drošas likvidēšanas procedūrām un obligātiem ekrāna bloķēšanas taimeriem.

11.4.4 CM-6 (Konfigurācijas iestatījumi) un IA-5 (Autentifikatoru pārvaldība): atbalsta ekrāna bloķēšanas un sesiju kontroles tehnisko piemērošanu galapunktos.

11.5 ES VDAR (2016/679)

11.5.1 Pants 5(1)(f): nosaka personas datu integritāti un konfidencialitāti, tostarp aizsardzību pret fizisku pakļaušanu riskam vai apskati no neatļautu personu puses.

11.5.2 32. pants – apstrādes drošība: nosaka pienākumu ieviest atbilstošus fiziskus un organizatoriskus pasākumus personas datu aizsardzībai pret nejaušu vai nelikumīgu iznīcināšanu, nozaudēšanu vai neatļautu izpaušanu; tas tiek nodrošināts ar galda un ekrāna kontroles pasākumiem.

11.5.3 Apsvērums 39: nosaka nepieciešamību ierobežot piekļuvi personas datiem tikai autorizētām personām; tas ietver arī to aizsardzību fiziskā formā, ja tie atstāti bez uzraudzības.

11.6 ES NIS2 direktīva (2022/2555)

11.6.1 Pants 21(2)(d): nosaka politikas un procedūras fiziskajai un vides drošībai, tostarp informācijas drošības aizsardzības pasākumiem darbvietu līmenī.

11.6.2 Pants 21(3): veicina drošības kultūru, kas ietver pareizu lietotāju uzvedību, informētību un nejaušas datu noplūdes novēršanu; to atbalsta šīs politikas uzvedības kontroles pasākumi.

11.7 ES DORA (2022/2554)

11.7.1 Pants 5 – Iekšējā pārvaldība un kontrole: nosaka, ka visi ar IKT saistītie riski, tostarp cilvēkfaktora un vides apdraudējumi, ir jāpārvalda ar piemērojamām politikām.

11.7.2 Pants 8 – IKT risku pārvaldība: nosaka aizsardzības pasākumus gan digitālajā, gan fiziskajā vidē, nodrošinot, ka attālināti lietotāji, filiāļu lietotāji un lietotāji uz vietas nerada nepārvaldītu pakļaušanu riskam.

11.7.3 Pants 9 – incidentu pārvaldība: nosaka, ka vides vai uzvedības trūkumi, kuru dēļ notikusi datu pakļaušana riskam, ir jāreģistrē, jāklasificē un jānovērš ar atbilstošām korektīvajām darbībām.

11.8 COBIT 2019

11.8.1 DSS01 – Pārvaldītas operācijas: nodrošina darbības disciplīnu fizisko darbvietu un sistēmu aizsardzībā, izmantojot atkārtojamus kontroles pasākumus.

11.8.2 DSS05 – Pārvaldīti drošības pakalpojumi: atbalsta datu, ierīču un piekļuves galapunktu aizsardzību ar uzvedībā balstītu politikas piemērošanu, piemēram, tīrā galda prasībām.

11.8.3 MEA03 – Atbilstības uzraudzība, izvērtēšana un novērtēšana: veicina fizisko aizsardzības pasākumu un politikas ieviešanas auditēšanu ikdienas darbības praksēs.