					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P09S					Dokumenta nosaukums: **Attālinātā darba 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 regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1., 6.2., 8. nodaļa	
ISO/IEC 27002:2022	6. kontrole	
NIST SP 800-53 Rev.5	AC-17, AC-2	
ES NIS2	21. panta 2. punkta b) un h) apakšpunkts	ES NIS2
ES DORA	9. pants	ES DORA
COBIT 2019	DSS05, APO13	COBIT 2019
ES GDPR	32. pants	ES GDPR

1. Mērķis

1.1 Šī politika nosaka drošības prasības darbiniekiem un līgumslēdzējiem, kuri strādā attālināti, tostarp no mājām, kopstrādes telpām vai komandējumu laikā.

1.2 Tās mērķis ir aizsargāt uzņēmuma informācijas konfidencialitāti, integritāti un pieejamību (CIA), kurai piekļūst ārpus uzņēmuma kontrolētajām vidēm.

1.3 Šī politika nodrošina atbilstību starptautiskajiem standartiem un mazina tādus riskus kā nesankcionēta piekļuve, datu zudums un pakalpojumu darbības traucējumi.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem personāla locekļiem (darbiniekiem, līgumslēdzējiem, konsultantiem un pagaidu darbiniekiem), kuri, strādājot ārpus uzņēmuma telpām, piekļūst uzņēmuma sistēmām, tīkliem vai datiem.

2.2 Tā aptver:

2.2.1 uzņēmuma izsniegtu un personīgo ierīču izmantošanu

2.2.2 piekļuvi, izmantojot VPN, attālo darbvirsmu vai mākoņpakalpojumus

2.2.3 drošu informācijas apstrādi ārpus uzņēmuma telpām

2.2.4 uzraudzību, izņēmumu pārvaldību un politikas ievērošanu

2.3 Tā attiecas gan uz pilna laika, gan nepilna laika attālinātā darba kārtību, tostarp ad hoc attālo piekļuvi.

3. Mērķi

3.1 Novērst nesankcionētu piekļuvi uzņēmuma sistēmām vai sensitīviem datiem attālinātā darba laikā.

3.2 Nodrošināt, ka ierīces un sakaru savienojumi, kas tiek izmantoti ārpus biroja, atbilst minimālajām drošības prasībām.

3.3 Uzturēt kontroli pār attālās piekļuves tiesībām un uzraudzību.

3.4 Nodrošināt skaidras vadlīnijas darbiniekiem un vadītājiem drošai attālinātā darba praksei.

3.5 Nodrošināt atbilstību ISO, NIS2, GDPR, DORA un COBIT prasībām attiecībā uz attālināto un mobilo darbu.

4. Lomas un pienākumi

4.1 Ģenerāldirektors

4.1.1 Apstiprina attālinātā darba kārtību un uzrauga atbilstību.

4.1.2 Eskalē drošības incidentus vai atkārtotu neatbilstību.

4.1.3 Pārskata izņēmumus un nodrošina turpmākās darbības pēc incidenta.

4.2 IT atbalsts vai ārējais IT pakalpojumu sniedzējs

4.2.1 Ievieš drošu attālo piekļuvi (piemēram, VPN, MFA).

4.2.2 Nodrošina galiekārtu aizsardzību, šifrēšanu un atbilstību ierīču konfigurācijas prasībām.

4.2.3 Atbalsta lietotājus un izmeklē visus tehniskās drošības jautājumus.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējā politikas pārskatīšana

9.1.1 Ģenerāldirektoram un IT atbalstam šī politika jāpārskata reizi gadā, lai nodrošinātu tās atbilstību tehnoloģiju, darba vides un tiesiskā regulējuma izmaiņām.

9.2 Priekšlaicīgas atjaunināšanas ierosinātāji

9.2.1 Nekavējoša pārskatīšana ir nepieciešama pēc:

9.2.1.1 būtiska attālinātā darba drošības incidenta

9.2.1.2 izmaiņām NIS2, GDPR vai DORA prasībās

9.2.1.3 pārejas uz jaunu attālās piekļuves tehnoloģiju (piemēram, citu VPN platformu)

9.3 Versiju kontrole un arhivēšana

9.3.1 Visām šīs politikas versijām jābūt:

9.3.1.1 datētām un ģenerāldirektora apstiprinātām

9.3.1.2 numurētām pa versijām

9.3.1.3 arhivētām vismaz trīs gadus

9.4 Personāla informēšana

9.4.1 Politikas atjauninājumi jāpaziņo visiem attālinātajiem lietotājiem. Jebkurām būtiskām izmaiņām ir nepieciešams iepazīšanās apliecinājums.

10. Saistītās politikas un sasaiste

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

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka, kurš autorizē un uzrauga attālo piekļuvi

10.1.2 P4S – Piekļuves kontroles politika: nosaka drošas attālās piekļuves ieviešanu un atsaukšanas procedūras

10.1.3 P6S – Risku pārvaldības politika: identificē un izvērtē riskus, kas saistīti ar piekļuvi ārpus uzņēmuma telpām

10.1.4 P8S – Informācijas drošības informētības un apmācības politika: apmāca lietotājus par attālinātā darba riskiem un labo praksi

10.1.5 P30S – Incidentu reaģēšanas politika: nosaka reaģēšanu uz attālās piekļuves incidentiem, piemēram, pieteikšanās datu noplūdi vai ierīces nozaudēšanu

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 6.1. punkts – uz risku balstīta plānošana attālās piekļuves scenārijiem

11.1.2 6.2. punkts – nosaka personāla funkcijas pienākumus mobilā un attālinātā darba kontekstā

11.1.3 8.1. punkts – attālo procesu darbības plānošana un kontrole

11.2 ISO/IEC 27002

11.2.1 6. kontrole – sniedz praktiskas vadlīnijas drošībai attālinātā un mobilā darba vidē

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – attālās piekļuves kontrole, sesiju aizsardzība un drošības uzraudzība

11.3.2 AC-2 – kontu pārvaldība lietotājiem ārpus uzņēmuma telpām

11.4 ES GDPR

11.4.1 32. pants – nosaka datu aizsardzības prasības, tostarp attālinātā darba vidē

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta b) apakšpunkts – nosaka drošu tīklu un informācijas sistēmu izmantošanu

11.5.2 21. panta 2. punkta h) apakšpunkts – paredz ar personālu saistītus drošības pasākumus, tostarp kontroles ārpus uzņēmuma telpām

11.6 ES DORA

11.6.1 9. pants – nosaka finanšu vienībām pienākumu uzturēt IKT noturību visos darbības režīmos, tostarp attālās piekļuves gadījumā

11.7 COBIT 2019

11.7.1 DSS05 – drošības pakalpojumu pārvaldība: ietver galiekārtu aizsardzību un droša attālinātā darba praksi

11.7.2 APO13 – pārvaldīta drošība: nodrošina drošas attālās un mobilās piekļuves piešķiršanu un risku uzraudzību