					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P09					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**

1. Mērķis

1.1 Šī politika nosaka obligātās prasības drošam attālinātajam darbam, tostarp organizācijas sistēmu izmantošanai, piekļuvei datiem un darba pienākumu izpildei ārpus uzņēmuma telpām.

1.2 Tā nodrošina attālināti pieejamo informācijas aktīvu konfidencialitāti, integritāti un pieejamību, kā arī nosaka kontroles pasākumus, lai mazinātu riskus, kas saistīti ar decentralizētu darba vidi.

1.3 Politika izpilda ISO/IEC 27001:2022 A pielikuma 6.7. kontroles prasības, ieviešot tehniskos un procesuālos drošības pasākumus, kas pielāgoti attālinātā darba apstākļiem.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visu personālu, kam ir atļauts strādāt attālināti, tostarp:

2.1.1 darbiniekiem (pilna laika, nepilna laika, uz līguma pamata);

2.1.2 ārējiem pakalpojumu sniedzējiem, konsultantiem un piegādātājiem;

2.1.3 pagaidu darbiniekiem un projektos iesaistītam personālam ar apstiprinātu attālo piekļuvi.

2.2 Tā aptver:

2.2.1 piekļuvi organizācijas sistēmām, izmantojot VPN vai apstiprinātus attālās piekļuves rīkus;

2.2.2 sensitīvas un regulētas informācijas apstrādi ārpus aizsargājamām telpām;

2.2.3 organizācijai piederoša aprīkojuma vai personīgo ierīču izmantošanu (BYOD);

2.2.4 fiziskos un loģiskos aizsardzības pasākumus attālinātā darba vidē.

2.3 Politika ir piemērojama visās valstīs un laika joslās, kur organizācija pieļauj attālināto darbu, neatkarīgi no tā, vai tas ir regulārs, ad hoc vai saistīts ar darbības nepārtrauktības notikumiem.

3. Mērķi

3.1 Nodrošināt, ka tikai autorizētas personas var attālināti piekļūt iekšējām sistēmām un informācijai.

3.2 Nodrošināt šifrēšanas, daudzfaktoru autentifikācijas (MFA) un galiekārtu aizsardzības piemērošanu visos attālās piekļuves kanālos.

3.3 Uzturēt drošības stāvokli pret tādiem apdraudējumiem kā pikšķerēšana, ļaunprogrammatūra, datu neatļauta iznese un nesankcionēta sistēmu eksponēšana.

3.4 Noteikt pārvaldības prasības tam, kā sensitīvie dati tiek pārsūtīti, glabāti vai drukāti ārpus organizācijas telpām.

3.5 Iekļaut fiziskās drošības pasākumus, kas samazina redzamības un nesankcionētas novērošanas risku attālinātu sesiju laikā.

3.6 Izpildīt starptautiskās regulatīvās prasības attiecībā uz attālinātu piekļuvi datiem, tostarp GDPR, NIS2 un DORA.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 apstiprina šo politiku un nodrošina, ka tās īstenošanai ir pieejami nepieciešamie resursi un tā ir integrēta personālvadības, IT un drošības operāciju procesos.

4.1.2 autorizē organizācijas attālinātā darba atbilstības kritērijus un piemērojamību struktūrvienībām.

4.2 Galvenais informācijas drošības vadītājs / IDPS vadītājs

4.2.1 ir politikas īpašnieks, uztur to un nodrošina tās atbilstību riska profilam un regulatīvajām prasībām.

4.2.2 nosaka drošības kontroles pasākumus attālajai piekļuvei (piemēram, šifrēšana, galiekārtu aizsardzība, sesiju noildze).

4.2.3 apstiprina izņēmumu pārvaldību un uzrauga kontroles pasākumu efektivitāti.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Pārskatīšanas biežums

9.1.1 Šī politika jāpārskata katru gadu vai biežāk, ja notiek:

9.1.1.1 jaunu attālās piekļuves tehnoloģiju ieviešana;

9.1.1.2 būtiska attālinātā darba paplašināšana (piemēram, hibrīdā darbaspēka iniciatīvas);

9.1.1.3 jaunu apdraudējumu, ievainojamību vai incidentu rašanās, kas saistīti ar attālināto vidi;

9.1.1.4 izmaiņas attiecīgajos tiesiskajos vai regulatīvajos ietvaros.

9.2 Īpašumtiesības un pārskatīšanas process

9.2.1 Politikas īpašnieks ir Galvenais informācijas drošības vadītājs. Pārskatīšana jāsaskaņo ar:

9.2.1.1 IT operācijām un arhitektūru;

9.2.1.2 personālvadības un objektu un aktīvu pārvaldības funkcijām (darbības un darba vietas ietekmes aspektiem);

9.2.1.3 datu aizsardzības speciālistu (privātuma un pārrobežu datu kontroles jautājumiem).

9.2.2 Politikas atjauninājumiem:

9.2.2.1 jābūt apstiprinātiem Informācijas drošības vadības komitejā;

9.2.2.2 jābūt paziņotiem visiem ietekmētajiem darbiniekiem un līgumslēdzējiem;

9.2.2.3 jābūt integrētiem personāla ievadapmācības un atkārtotas apmācības materiālos.

9.3 Dokumentu kontrole un izplatīšana

9.3.1 Politikā jāiekļauj versiju kontrole, spēkā stāšanās datums un izmaiņu vēsture.

9.3.2 Aizstātās versijas jāglabā saskaņā ar Dokumentu pārvaldības politiku (P14).

9.3.3 Pārskatītām versijām jāparedz obligāta atkārtota iepazīšanās apliecinājuma sniegšana lietotājiem, kam ir atļauts strādāt attālināti.

10. Saistītās politikas un sasaiste

10.1 Šī politika darbojas kopā ar:

10.1.1 P1 – Informācijas drošības politika: nosaka drošas aktīvu apstrādes pamatprincipus, kas piemērojami visās darba vidēs, tostarp attālinātajā darbā.

10.1.2 P3 – Pieļaujamās lietošanas politika: nosaka organizācijas ierīču un sistēmu atbilstošu izmantošanu attālinātā darba sesiju laikā.

10.1.3 P4 – Piekļuves kontroles politika: nodrošina, ka attālās piekļuves privilēģijas ievēro minimāli nepieciešamo tiesību principu un atbilstošus autentifikācijas mehānismus.

10.1.4 P6 – Risku pārvaldības politika: nosaka, kā attālinātā darba riski tiek identificēti, apstrādāti un uzraudzīti IDPS ietvarā.

10.1.5 P12 – Aktīvu pārvaldības politika: nosaka pienākumu veikt visu attālināti izmantoto ierīču uzskaiti un konfigurācijas pārvaldību.

10.1.6 P22 – Žurnalēšanas un uzraudzības politika: nodrošina, ka attālinātās sesijas tiek uzraudzītas, auditētas un glabātas atbilstoši atbilstības prasībām.

10.1.7 P14 – Datu uzglabāšanas un likvidēšanas politika: nosaka datu apstrādes noteikumus, kas attiecas uz attālināto darbu, tostarp noņemamajiem datu nesējiem un ierīču likvidēšanu.

10.2 Šīs politikas kopumā nodrošina, ka attālinātais darbs ir drošs, atbilstošs un piemērojams visās funkcijās un valstīs.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem drošības, datu aizsardzības un IKT risku pārvaldības ietvariem, lai nodrošinātu drošu, izsekojamu un atbilstošu attālinātā darba praksi.

11.2 ISO/IEC 27001

11.2.1 Punkts 6.1.3 – Risku apstrādes plānošana: šī politika veicina ar attālo piekļuvi un decentralizētu darba vidi saistīto risku apstrādi.

11.2.2 Punkts 8.1 – Darbību plānošana un kontrole: prasa ieviest kontroles pasākumus sistēmām, kurām piekļūst ārpus organizācijas telpām.

11.2.3 A pielikuma 6.7. kontrole – Attālinātais darbs: šī politika pilnībā aptver nepieciešamos informācijas drošības kontroles pasākumus, kad personāls strādā ārpus organizācijas telpām, tostarp fiziskos un loģiskos aizsardzības pasākumus, piekļuves pārvaldību un lietotāju rīcības uzraudzību.

11.3 ISO/IEC 27002:2022 – 6. kontrole

11.3.1 Šī kontrole nosaka procesuālos un tehniskos drošības pasākumus attālinātam darbam. Tā ietver prasības attiecībā uz ierīču drošību, piekļuves metodēm, datu apstrādi, vides aizsardzības pasākumiem un trešo pušu dalībnieku pārvaldību — to visu nodrošina šī politika.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Attālā piekļuve): tieši nodrošināta ar VPN kontroles pasākumiem, MFA, sesiju žurnalēšanu un attālināto lietotāju lomu balstītu piekļuves autorizāciju.

11.4.2 AC-2 (Kontu pārvaldība): kontrolē piekļuves atbilstību, attālināto privilēģiju piešķiršanu un kontu deaktivizāciju.

11.4.3 SC-12 līdz SC-13 (Kriptogrāfiskā aizsardzība, kriptogrāfisko atslēgu izveide): ieviestas, obligāti izmantojot VPN un pilna diska šifrēšanu attālinātajām galiekārtām.

11.4.4 MP-5 (Datu nesēju pārvadāšanas aizsardzība) un PE-18 (Informācijas sistēmu komponentu atrašanās vieta): attālinātā darba vadlīnijas nosaka pārvadāšanas aizsardzību un fiziskos drošības pasākumus ārpus uzņēmuma telpām.

11.4.5 AU-2, AU-6: attālināto sesiju žurnalēšana un uzraudzība atbalsta audita un incidentu reaģēšanas prasības.

11.5 ES GDPR (2016/679)

11.5.1 32. pants – apstrādes drošība: šī politika piemēro attālās piekļuves drošības, šifrēšanas un žurnalēšanas kontroles pasākumus, kas nepieciešami, lai aizsargātu personas datus, kuriem piekļūst vai kurus apstrādā attālināti.

11.5.2 5. panta 1. punkta f) apakšpunkts: nodrošina, ka personas dati, kuriem piekļūst ārpus uzņēmuma telpām, ir aizsargāti pret nesankcionētu vai nelikumīgu apstrādi un nejaušu zudumu.

11.5.3 Apsvērums 39: uzsver piekļuves ierobežošanu, integritāti un konfidencialitāti — īpaši būtiski, kad ierīces tiek iznestas no aizsargājamām telpām.

11.6 ES NIS2 direktīva (2022/2555)

11.6.1 21. panta 2. punkta a), b), d) apakšpunkts: prasa nodrošināt attālās piekļuves drošību kā daļu no organizācijas IKT risku pārvaldības ietvara. Šī politika izpilda prasību par drošības pasākumiem, kas aptver piekļuves kontroli, datu drošību un organizatoriskās politikas attālinātām vidēm.

11.6.2 21. panta 3. punkts: veicina drošības izpratni un politikas ievērošanu personālam, kas strādā ārpus centrālajām telpām.

11.7 ES DORA (2022/2554)

11.7.1 5. pants – Pārvaldības un iekšējās kontroles ietvars: šī politika atbalsta IKT riska kontroles prasības visos darbības scenārijos, tostarp hibrīdajos un attālinātajos modeļos.

11.7.2 8. pants – IKT risku pārvaldības ietvars: attālās piekļuves riski tiek identificēti, mazināti un pārvaldīti, izmantojot šeit noteiktos tehniskos un organizatoriskos kontroles pasākumus.

11.7.3 9. pants – Informācijas apmaiņas kārtība: aizsargā pret attālinātu informācijas noplūdi digitālās operacionālās noturības tīklos kopīgotai informācijai.

11.8 COBIT 2019

11.8.1 DSS01 – Pārvaldītas operācijas: šī politika atbalsta drošu darbības nepārtrauktību neatkarīgi no fiziskās atrašanās vietas.

11.8.2 BAI06 – Pārvaldītas IT izmaiņas un BAI09 – Pārvaldīti aktīvi: nodrošina, ka attālinātā darba ierīces tiek uzskaitītas, droši konfigurētas un pārvaldītas kā kritiski aktīvi.

11.8.3 APO13 – Pārvaldīta drošība: veicina noteiktu drošības pārvaldības ietvaru attālinātām vidēm.

11.8.4 MEA03 – Uzraudzīt, izvērtēt un novērtēt atbilstību: nosaka, ka attālinātā darba aktivitātes ir jāreģistrē žurnālos, jāpārskata un jāauditē.