					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P09					Naslov dokumenta: **Politika dela na daljavo**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

1. Namen

1.1 Ta politika določa obvezne zahteve za varno izvajanje dela na daljavo, vključno z uporabo informacijskih sistemov organizacije, dostopom do podatkov in izvajanjem delovnih nalog zunaj prostorov podjetja.

1.2 Zagotavlja zaupnost, celovitost in razpoložljivost (CIA) informacijskih sredstev, do katerih se dostopa na daljavo, ter določa kontrole za zmanjševanje tveganj, povezanih z razpršenimi delovnimi okolji.

1.3 Politika izpolnjuje zahteve Priloge A, kontrole 6.7 standarda ISO/IEC 27001:2022 z uvedbo tehničnih in postopkovnih varovalnih ukrepov, prilagojenih pogojem dela na daljavo.

2. Področje uporabe

2.1 Ta politika velja za vse osebe, ki so pooblaščene za delo na daljavo, vključno z:

2.1.1 zaposlenimi (za polni delovni čas, krajši delovni čas ali po pogodbi)

2.1.2 zunanjimi izvajalci, svetovalci in dobavitelji

2.1.3 začasnimi in projektnimi sodelavci z odobrenim oddaljenim dostopom

2.2 Politika zajema:

2.2.1 dostop do informacijskih sistemov organizacije prek VPN ali odobrenih orodij za oddaljeni dostop

2.2.2 ravnanje z občutljivimi in reguliranimi informacijami zunaj varovanih prostorov

2.2.3 uporabo opreme v lasti organizacije ali uporabo zasebnih naprav

2.2.4 fizične in logične zaščitne ukrepe v oddaljenih okoljih

2.3 Politika se uporablja na vseh geografskih območjih in v vseh časovnih pasovih, kjer organizacija dovoljuje delo na daljavo, bodisi redno, ad hoc ali med dogodki, povezanimi z neprekinjenim poslovanjem.

3. Cilji

3.1 Zagotoviti, da lahko do notranjih sistemov in informacij na daljavo dostopajo samo pooblaščene osebe.

3.2 Zahtevati šifriranje, večfaktorsko avtentikacijo (MFA) in zaščito končnih točk na vseh poteh oddaljenega dostopa.

3.3 Ohranjati varno raven tveganja na področju informacijske varnosti pred grožnjami, kot so napadi z lažnim predstavljanjem, zlonamerna programska oprema, odtekanje podatkov in nepooblaščena izpostavljenost sistemov.

3.4 Določiti pravila za prenos, shranjevanje in tiskanje občutljivih podatkov v okoljih zunaj lokacije.

3.5 Vzpostaviti ukrepe fizičnega varovanja, ki zmanjšujejo vidnost in možnost nepooblaščenega opazovanja med oddaljenimi sejami.

3.6 Zagotoviti skladnost z mednarodnimi regulativnimi zahtevami glede oddaljenega dostopa do podatkov, vključno z GDPR, NIS2 in DORA.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri to politiko ter zagotovi ustrezne vire in njeno vključitev v kadrovske procese, delovanje IT in varnostne operacije.

4.1.2 Odobri merila upravičenosti do dela na daljavo na ravni organizacije in uporabo po poslovnih enotah.

4.2 Vodja informacijske varnosti / vodja ISMS

4.2.1 Je nosilec politike, skrbi za njeno vzdrževanje in usklajenost s profilom tveganja ter regulativnimi zahtevami.

4.2.2 Določi varnostne kontrole za oddaljeni dostop (npr. šifriranje, zaščita končnih točk, časovne omejitve sej).

4.2.3 Odobrava obravnavo izjem in spremlja učinkovitost kontrol.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 Pogostost pregledov

9.1.1 To politiko je treba pregledati letno ali pogosteje ob:

9.1.1.1 uvedbi novih tehnologij za oddaljeni dostop

9.1.1.2 pomembni razširitvi dela na daljavo (npr. pobude za hibridni način dela)

9.1.1.3 pojavu novih groženj, ranljivosti ali incidentov, povezanih z oddaljenimi okolji

9.1.1.4 spremembah ustreznih pravnih ali regulativnih okvirov

9.2 Lastništvo in postopek pregleda

9.2.1 Nosilec politike je vodja informacijske varnosti. Pregled se mora usklajevati z:

9.2.1.1 IT operacijami in arhitekturo

9.2.1.2 kadrovsko službo in službo za upravljanje prostorov (zaradi operativnih posledic in vplivov na delovni prostor)

9.2.1.3 pooblaščeno osebo za varstvo podatkov (DPO) (zaradi zasebnosti in kontrol čezmejnega prenosa podatkov)

9.2.2 Posodobitve politike morajo biti:

9.2.2.1 odobrene s strani usmerjevalnega odbora ISMS

9.2.2.2 sporočene vsem zadevnim zaposlenim in pogodbenim izvajalcem

9.2.2.3 vključene v gradiva za uvajanje in obnovitveno usposabljanje

9.3 Nadzor dokumenta in distribucija

9.3.1 Politika mora vključevati upravljanje različic, datum začetka veljavnosti in evidenco sprememb.

9.3.2 Nadomeščene različice je treba hraniti v skladu s Politiko upravljanja dokumentacije (P14).

9.3.3 Revidirane različice morajo sprožiti obvezno ponovno potrditev za uporabnike, upravičene do dela na daljavo.

10. Povezane politike in povezave

10.1 Ta politika deluje skupaj z naslednjimi politikami:

10.1.1 P1 – Politika informacijske varnosti: določa osnovni okvir za varno ravnanje s sredstvi, ki velja za vsa delovna okolja, vključno z delom na daljavo.

10.1.2 P3 – Politika sprejemljive uporabe (AUP): ureja ustrezno uporabo naprav in sistemov organizacije med sejami dela na daljavo.

10.1.3 P4 – Politika nadzora dostopa: zagotavlja, da privilegiji oddaljenega dostopa sledijo načelu najmanjših privilegijev in ustreznim mehanizmom avtentikacije.

10.1.4 P6 – Politika upravljanja tveganj: določa, kako se tveganja dela na daljavo identificirajo, obravnavajo in spremljajo v okviru ISMS.

10.1.5 P12 – Politika upravljanja sredstev: zahteva popis sredstev in upravljanje konfiguracije za vse naprave, ki se uporabljajo na daljavo.

10.1.6 P22 – Politika beleženja in spremljanja: zagotavlja, da so oddaljene seje spremljane, revidirane in hranjene v skladu z zahtevami skladnosti.

10.1.7 P14 – Politika hrambe in odstranjevanja podatkov: določa pravila ravnanja s podatki, pomembna za delo na daljavo, vključno z izmenljivimi mediji in odstranjevanjem naprav.

10.2 Te politike skupaj zagotavljajo, da je delo na daljavo varno, skladno in izvršljivo v vseh funkcijah in na vseh geografskih območjih.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi okviri za varnost, varstvo podatkov in upravljanje tveganj IKT, da zagotovi varne, sledljive in skladne prakse dela na daljavo.

11.2 ISO/IEC 27001

11.2.1 Klavzula 6.1.3 – načrtovanje obravnave tveganj: ta politika prispeva k obravnavi tveganj, povezanih z oddaljenim dostopom in razpršenimi delovnimi okolji.

11.2.2 Klavzula 8.1 – operativno načrtovanje in nadzor: zahteva izvajanje kontrol za sisteme, do katerih se dostopa zunaj prostorov organizacije.

11.2.3 Priloga A, kontrola 6.7 – delo na daljavo: ta politika v celoti obravnava zahtevane kontrole informacijske varnosti, kadar osebje dela zunaj prostorov organizacije, vključno s fizičnimi in logičnimi zaščitnimi ukrepi, upravljanjem pravic dostopa in spremljanjem vedenja uporabnikov.

11.3 ISO/IEC 27002:2022 – Kontrola 6

11.3.1 Ta kontrola zahteva postopkovne in tehnične varovalne ukrepe za delo na daljavo. Vključuje zahteve glede varnosti naprav, načinov dostopa, ravnanja s podatki, okoljskih varovalnih ukrepov in upravljanja tretjih oseb, kar se uveljavlja s to politiko.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (oddaljeni dostop): neposredno podprto s kontrolami VPN, MFA, beleženjem sej v dnevnike in odobravanjem oddaljenega dostopa na podlagi vlog.

11.4.2 AC-2 (upravljanje računov): nadzira upravičenost dostopa, dodeljevanje oddaljenih privilegijev in deaktivacijo računov.

11.4.3 SC-12 do SC-13 (kriptografska zaščita, vzpostavljanje kriptografskih ključev): izvedeno z obvezno uporabo VPN in šifriranjem celotnega diska za oddaljene končne točke.

11.4.4 MP-5 (zaščita prenosa medijev) in PE-18 (lokacija komponent informacijskega sistema): smernice za delo na daljavo zahtevajo zaščito prenosa in fizične varovalne ukrepe v okoljih zunaj lokacije.

11.4.5 AU-2, AU-6: beleženje in spremljanje oddaljenih sej podpira zahteve glede revizije in odzivanja na incidente.

11.5 Uredba EU GDPR (2016/679)

11.5.1 Člen 32 – varnost obdelave: ta politika uveljavlja kontrole varnosti oddaljenega dostopa, šifriranja in beleženja v dnevnike, potrebne za zaščito osebnih podatkov, do katerih se dostopa ali se obdelujejo na daljavo.

11.5.2 Člen 5(1)(f): zagotavlja, da so osebni podatki, do katerih se dostopa zunaj lokacije, zaščiteni pred nepooblaščeno ali nezakonito obdelavo ter nenamerno izgubo.

11.5.3 Uvodna izjava 39: poudarja omejevanje dostopa, celovitost in zaupnost, zlasti kadar naprave zapustijo varovane prostore.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Člen 21(2)(a, b, d): zahteva, da je oddaljeni dostop zavarovan kot del organizacijskega okvira za upravljanje tveganj IKT. Ta politika izpolnjuje zahteve za varnostne ukrepe, ki zajemajo nadzor dostopa, varnost podatkov in organizacijske politike za oddaljena okolja.

11.6.2 Člen 21(3): spodbuja varnostno ozaveščanje in izvajanje politike med zaposlenimi, ki delajo zunaj osrednjih prostorov.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Člen 5 – okvir upravljanja in notranjih kontrol: ta politika podpira pričakovanja glede obvladovanja tveganj IKT v vseh operativnih scenarijih, vključno s hibridnimi in oddaljenimi modeli.

11.7.2 Člen 8 – okvir upravljanja tveganj IKT: tveganja oddaljenega dostopa so identificirana, zmanjšana in upravljana s tehničnimi in organizacijskimi kontrolami, določenimi v tej politiki.

11.7.3 Člen 9 – ureditve za izmenjavo informacij: ščiti pred oddaljenim odtekanjem informacij, ki se delijo znotraj omrežij digitalne operativne odpornosti.

11.8 COBIT 2019

11.8.1 DSS01 – upravljane operacije: ta politika podpira varno neprekinjeno poslovanje ne glede na fizično lokacijo.

11.8.2 BAI06 – upravljane spremembe IT in BAI09 – upravljana sredstva: zagotavljata, da so naprave za delo na daljavo sledene, varno konfigurirane in obravnavane kot kritična sredstva.

11.8.3 APO13 – upravljana varnost: spodbuja opredeljen okvir upravljanja varnosti za oddaljena okolja.

11.8.4 MEA03 – spremljanje, vrednotenje in presoja skladnosti: določa, da morajo biti dejavnosti dela na daljavo beležene v dnevnike, pregledovane in revidirane.