| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P09S | | | | | Naslov dokumenta:<br>**Politika dela na daljavo** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>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** |
| | | | |
| | | | |

**Pravno obvestilo (avtorske pravice in omejitve uporabe)**

(C) 2025 Clarysec LLC. All rights reserved.

Ta dokument je intelektualna lastnina družbe Clarysec LLC. Noben del tega dokumenta se ne sme kopirati, ponovno uporabiti, distribuirati ali spreminjati za komercialne ali implementacijske namene brez predhodnega izrecnega pisnega dovoljenja.

Nepooblaščena uporaba je strogo prepovedana in lahko povzroči pravne ukrepe.

Za licenciranje se obrnite na: info@clarysec.com

Usklajeno s standardi in predpisi

| Standard/predpis | Klavzula/člen | Komentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klavzule 6.1, 6.2, 8 | |
| ISO/IEC 27002:2022 | Kontrola 6 | |
| NIST SP 800-53 Rev.5 | AC-17, AC-2 | |
| Direktiva EU NIS2 | Člena 21(2)(b), 21(2)(h) | EU NIS2 |
| Uredba EU DORA | Člen 9 | EU DORA |
| COBIT 2019 | DSS05, APO13 | COBIT 2019 |
| Uredba EU GDPR | Člen 32 | EU GDPR |

**1. Namen**

1.1 Ta politika določa varnostne zahteve za zaposlene in pogodbene izvajalce, ki delajo na daljavo, vključno z delom od doma, v skupnih delovnih prostorih ali med potovanjem.

1.2 Njen namen je varovati zaupnost, celovitost in razpoložljivost (CIA) poslovnih informacij, do katerih se dostopa zunaj okolij, ki so pod nadzorom podjetja.

1.3 Ta politika zagotavlja skladnost z mednarodnimi standardi ter zmanjšuje tveganja, kot so nepooblaščen dostop, izguba podatkov in prekinitev storitev.

**2. Področje uporabe**

2.1 Ta politika velja za vse člane osebja (zaposlene, pogodbene izvajalce, svetovalce in začasne delavce), ki pri delu zunaj lokacije dostopajo do sistemov, omrežij ali podatkov podjetja.

**2.2 Zajema:**

2.2.1 uporabo naprav podjetja in naprav v osebni lasti

2.2.2 dostop prek VPN, oddaljenega namizja ali storitev v oblaku

2.2.3 varno ravnanje z informacijami zunaj prostorov podjetja

2.2.4 spremljanje, obravnavo izjem in izvajanje te politike

2.3 Velja za stalne in občasne oblike dela na daljavo, vključno z ad hoc oddaljenim dostopom.

**3. Cilji**

3.1 Preprečiti nepooblaščen dostop do sistemov podjetja ali občutljivih podatkov med delom na daljavo.

3.2 Zagotoviti, da naprave in komunikacijske povezave, ki se uporabljajo zunaj pisarne, izpolnjujejo osnovne varnostne zahteve.

3.3 Ohraniti nadzor nad pravicami oddaljenega dostopa in spremljanjem.

3.4 Zaposlenim in vodjem zagotoviti jasne usmeritve za varne prakse dela na daljavo.

3.5 Izpolnjevati zahteve standardov in okvirov ISO, NIS2, GDPR, DORA in COBIT za delo na daljavo in mobilno delo.

**4. Vloge in odgovornosti**

**4.1 Generalni direktor**

4.1.1 Odobri ureditev dela na daljavo in spremlja skladnost.

4.1.2 Eskalira varnostne incidente ali ponavljajočo se neskladnost.

4.1.3 Pregleduje izjeme in zagotavlja nadaljnje ukrepanje po incidentih.

**4.2 IT podpora ali zunanji izvajalec IT-storitev**

4.2.1 Vzpostavi varen oddaljeni dostop (npr. VPN, MFA).

4.2.2 Zagotavlja varnost končnih točk, šifriranje in varne konfiguracije naprav.

4.2.3 Podpira uporabnike in preiskuje tehnične varnostne težave.

[ ... 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 Letni pregled politike**

9.1.1 Generalni direktor in IT podpora morata to politiko pregledati najmanj enkrat letno, da ostane usklajena s tehnološkimi, kadrovskimi in pravnimi spremembami.

**9.2 Sprožilci za predčasno posodobitev**

**9.2.1 Takojšnji pregled je zahtevan po:**

9.2.1.1 večjem varnostnem incidentu pri delu na daljavo

9.2.1.2 spremembah zahtev NIS2, GDPR ali DORA

9.2.1.3 prehodu na novo tehnologijo oddaljenega dostopa (npr. drugo platformo VPN)

**9.3 Upravljanje različic in arhiviranje**

**9.3.1 Vse različice te politike morajo biti:**

9.3.1.1 datirane in odobrene s strani generalnega direktorja

9.3.1.2 označene s številko različice

9.3.1.3 arhivirane najmanj tri leta

**9.4 Obveščanje osebja**

9.4.1 O posodobitvah te politike je treba obvestiti vse oddaljene uporabnike. Za vsako pomembno spremembo je zahtevana potrditev.

**10. Povezane politike in povezave**

**10.1 Ta politika je povezana z naslednjimi dokumenti in jih podpira:**

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa, kdo odobri in nadzira oddaljeni dostop

10.1.2 P4S – Politika nadzora dostopa: določa postopke za varno vzpostavitev in preklic oddaljenega dostopa

10.1.3 P6S – Politika obvladovanja tveganj: evidentira in ocenjuje tveganja, povezana z dostopom zunaj lokacije

10.1.4 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: usposablja uporabnike glede tveganj dela na daljavo in dobrih praks

10.1.5 P30S – Politika odzivanja na incidente: ureja odziv na incidente pri oddaljenem dostopu, kot so razkritje poverilnic ali izguba naprave

**11. Referenčni standardi in okviri**

**11.1 ISO/IEC 27001**

11.1.1 Klavzula 6.1 – načrtovanje na podlagi tveganj za scenarije oddaljenega dostopa

11.1.2 Klavzula 6.2 – obravnava odgovornosti kadrovske službe v mobilnih oziroma oddaljenih okoliščinah

11.1.3 Klavzula 8.1 – operativno načrtovanje in nadzor oddaljenih procesov

**11.2 ISO/IEC 27002**

11.2.1 Kontrola 6.7 – podaja praktične usmeritve za varnost pri delu na daljavo in mobilnem delu

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AC-17 – nadzor oddaljenega dostopa, zaščita sej in spremljanje varnosti

11.3.2 AC-2 – upravljanje uporabniških računov za uporabnike zunaj lokacije

**11.4 Uredba EU GDPR**

11.4.1 Člen 32 – zahteva varstvo podatkov »že pri načrtovanju in privzeto«, tudi v oddaljenih okoljih

**11.5 Direktiva EU NIS2**

11.5.1 Člen 21(2)(b) – zahteva varno uporabo omrežnih in informacijskih sistemov

11.5.2 Člen 21(2)(h) – določa kadrovske varnostne ukrepe, vključno s kontrolami zunaj lokacije

**11.6 Uredba EU DORA**

11.6.1 Člen 9 – od finančnih subjektov zahteva vzdrževanje odpornosti sistemov IKT v vseh načinih delovanja, vključno z oddaljenim dostopom

**11.7 COBIT 2019**

11.7.1 DSS05 – upravljanje varnostnih storitev: vključuje zaščito končnih točk in varne prakse dela na daljavo

11.7.2 APO13 – upravljana varnost: zagotavlja varno dodeljevanje in nadzor tveganj pri mobilnem oziroma oddaljenem dostopu