					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P09S					Naziv dokumenta: **Politika rada na daljinu**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrola 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
EU NIS2	Članci 21(2)(b), 21(2)(h)	EU NIS
EU DORA	Članak 9	EU DORA
COBIT 2019	DSS05, APO13	COBIT 2019
EU GDPR	Članak 32	EU GDPR

1. Svrha

1.1 Ova politika utvrđuje sigurnosne zahtjeve za zaposlenike i ugovorne izvođače koji rade na daljinu, uključujući rad od kuće, iz dijeljenih radnih prostora ili tijekom putovanja.

1.2 Svrha ove politike je zaštita povjerljivosti, cjelovitosti i dostupnosti poslovnih informacija kojima se pristupa izvan okruženja pod kontrolom organizacije.

1.3 Ova politika osigurava usklađenost s međunarodnim standardima i smanjuje rizike kao što su neovlašteni pristup, gubitak podataka i prekid usluga.

2. Područje primjene

2.1 Ova se politika primjenjuje na sve članove osoblja (zaposlenike, ugovorne izvođače, konzultante i privremene radnike) koji pristupaju sustavima, mrežama ili podacima organizacije tijekom rada izvan lokacije.

2.2 Obuhvaća:

2.2.1 uporabu uređaja koje je osigurala organizacija i osobnih uređaja

2.2.2 pristup putem VPN-a, udaljene radne površine ili usluga u oblaku

2.2.3 sigurno rukovanje informacijama izvan prostorija organizacije

2.2.4 praćenje, postupanje s iznimkama i provedbu

2.3 Primjenjuje se na rad na daljinu s punim i nepunim radnim vremenom, uključujući ad hoc udaljeni pristup.

3. Ciljevi

3.1 Spriječiti neovlašteni pristup sustavima organizacije ili osjetljivim podacima tijekom rada na daljinu.

3.2 Osigurati da uređaji i komunikacijske veze koji se upotrebljavaju izvan ureda ispunjavaju zahtjeve sigurnosne osnovne konfiguracije.

3.3 Održavati kontrolu nad pristupnim ovlastima za udaljeni pristup i nadzorom.

3.4 Osigurati jasne smjernice zaposlenicima i rukovoditeljima za sigurne prakse rada na daljinu.

3.5 Ispuniti zahtjeve standarda ISO, NIS2, GDPR, DORA i COBIT koji se odnose na rad na daljinu i mobilni rad.

4. Uloge i odgovornosti

4.1 Nadređeni rukovoditelj

4.1.1 Odobrava aranžmane rada na daljinu i prati usklađenost.

4.1.2 Eskalira sigurnosne incidente ili ponovljenu neusklađenost.

4.1.3 Pregledava iznimke i osigurava daljnje postupanje nakon incidenta.

4.2 IT podrška ili vanjski pružatelj IT usluga

4.2.1 Uspostavlja siguran udaljeni pristup (npr. VPN, višefaktorska autentifikacija (MFA)).

4.2.2 Osigurava sigurnost krajnjih točaka, šifriranje i konfiguraciju uređaja.

4.2.3 Pruža korisničku podršku i istražuje sve tehničke sigurnosne probleme.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Godišnji pregled politike

9.1.1 Nadređeni rukovoditelj i IT podrška moraju najmanje jednom godišnje pregledati ovu politiku radi usklađivanja s tehnološkim, kadrovskim i pravnim promjenama.

9.2 Okidači za ranije ažuriranje

9.2.1 Neposredan pregled obvezan je nakon:

9.2.1.1 velikog sigurnosnog incidenta povezanog s radom na daljinu

9.2.1.2 promjene zahtjeva NIS2, GDPR-a ili DORA-e

9.2.1.3 prelaska na novu tehnologiju udaljenog pristupa (npr. drugu VPN platformu)

9.3 Upravljanje verzijama i arhiviranje

9.3.1 Sve verzije ove politike moraju biti:

9.3.1.1 datirane i odobrene od strane nadređenog rukovoditelja

9.3.1.2 označene brojem verzije

9.3.1.3 arhivirane najmanje tri godine

9.4 Komunikacija osoblju

9.4.1 Ažuriranja politike moraju se priopćiti svim udaljenim korisnicima. Za svaku značajnu promjenu potrebna je potvrda upoznatosti.

10. Povezane politike i poveznice

10.1 Ova je politika povezana sa sljedećim dokumentima i pruža im podršku:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: definira tko odobrava i nadzire udaljeni pristup

10.1.2 P4S – Politika kontrole pristupa: utvrđuje sigurno uspostavljanje udaljenog pristupa i postupke ukidanja prava pristupa

10.1.3 P6S – Politika upravljanja rizicima: prati i vrednuje rizike povezane s pristupom izvan lokacije

10.1.4 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osposobljava korisnike o rizicima rada na daljinu i dobrim praksama

10.1.5 P30S – Politika odgovora na incidente: uređuje odgovor na incidente udaljenog pristupa kao što su kompromitacija vjerodajnica ili gubitak uređaja

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1 – planiranje temeljeno na riziku za scenarije udaljenog pristupa

11.1.2 Točka 6.2 – uređuje odgovornosti ljudskih resursa (HR) u mobilnim i udaljenim kontekstima

11.1.3 Točka 8.1 – operativno planiranje i kontrola udaljenih procesa

11.2 ISO/IEC 27002

11.2.1 Kontrola 6.7 – pruža praktične smjernice o sigurnosti za rad na daljinu i mobilni rad

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – kontrola udaljenog pristupa, zaštita sesija i sigurnosni nadzor

11.3.2 AC-2 – upravljanje računima za korisnike izvan lokacije

11.4 EU GDPR

11.4.1 Članak 32 – zahtijeva zaštitu podataka „ugrađeno i prema zadanim postavkama”, uključujući i u udaljenim okruženjima

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(b) – zahtijeva sigurnu uporabu mrežnih i informacijskih sustava

11.5.2 Članak 21(2)(h) – zahtijeva sigurnosne mjere povezane s ljudskim resursima, uključujući kontrole izvan lokacije

11.6 EU DORA

11.6.1 Članak 9 – zahtijeva da financijski subjekti održavaju otpornost IKT-a u svim načinima rada, uključujući udaljeni pristup

11.7 COBIT 2019

11.7.1 DSS05 – Upravljanje sigurnosnim uslugama: uključuje zaštitu krajnjih točaka i sigurne prakse rada na daljinu

11.7.2 APO13 – Upravljana sigurnost: osigurava sigurnu dodjelu pristupa i nadzor rizika za mobilni i udaljeni pristup