					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P09					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**

1. Svrha

1.1 Ova politika utvrđuje obvezne zahtjeve za sigurno obavljanje rada na daljinu, uključujući uporabu organizacijskih sustava, pristup podacima i izvršavanje radnih obveza izvan poslovnih prostora društva.

1.2 Njome se osiguravaju povjerljivost, cjelovitost i dostupnost informacijskih resursa kojima se pristupa na daljinu te uspostavljaju kontrole za smanjenje rizika povezanih s distribuiranim radnim okruženjima.

1.3 Ova politika ispunjava zahtjeve kontrole 6.7 iz Priloga A norme ISO/IEC 27001:2022 provedbom tehničkih i organizacijskih zaštitnih mjera prilagođenih uvjetima rada na daljinu.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve osobe ovlaštene za rad na daljinu, uključujući:

2.1.1 zaposlenike (puno radno vrijeme, nepuno radno vrijeme, ugovorni angažman)

2.1.2 vanjske pružatelje usluga, konzultante i dobavljače

2.1.3 privremeno i projektno angažirano osoblje s odobrenim udaljenim pristupom

2.2 Ova politika obuhvaća:

2.2.1 pristup organizacijskim sustavima putem VPN-a ili odobrenih alata za udaljeni pristup

2.2.2 rukovanje osjetljivim i reguliranim informacijama izvan sigurnih prostora

2.2.3 uporabu opreme u vlasništvu organizacije ili osobnih uređaja (BYOD)

2.2.4 fizičke i logičke zaštitne mjere u udaljenim okruženjima

2.3 Ova politika primjenjuje se u svim zemljopisnim područjima i vremenskim zonama u kojima organizacija dopušta rad na daljinu, bilo redovito, povremeno ili tijekom događaja povezanih s kontinuitetom poslovanja.

3. Ciljevi

3.1 Osigurati da samo ovlaštene osobe mogu na daljinu pristupati internim sustavima i informacijama.

3.2 Osigurati primjenu enkripcije, višefaktorske autentikacije (MFA) i zaštite krajnjih uređaja na svim kanalima udaljenog pristupa.

3.3 Održavati razinu sigurnosti otpornu na prijetnje kao što su phishing, zlonamjerni softver, iznošenje podataka i neovlaštena izloženost sustava.

3.4 Urediti način prijenosa, pohrane i ispisa osjetljivih podataka u okruženjima izvan lokacija organizacije.

3.5 Uspostaviti mjere fizičke sigurnosti koje smanjuju vidljivost i rizik od neovlaštenog promatranja tijekom udaljenih sesija.

3.6 Osigurati usklađenost s međunarodnim regulatornim zahtjevima koji se odnose na udaljeni pristup podacima, uključujući GDPR, NIS2 i DORA.

4. Uloge i odgovornosti

4.1 Izvršno rukovodstvo

4.1.1 Odobrava ovu politiku te osigurava potrebne resurse i njezinu integraciju u HR, IT i sigurnosne operacije.

4.1.2 Odobrava kriterije prihvatljivosti za rad na daljinu i primjenjivost po organizacijskim jedinicama.

4.2 CISO / voditelj ISMS-a

4.2.1 Odgovoran je za ovu politiku, njezino održavanje i usklađenost s razinom rizika i regulatornim zahtjevima.

4.2.2 Definira sigurnosne kontrole za udaljeni pristup (npr. enkripcija, zaštita krajnjih uređaja, vremenska ograničenja sesije).

4.2.3 Odobrava postupanje s iznimkama i prati učinkovitost kontrola.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Učestalost pregleda

9.1.1 Ova politika mora se pregledati jednom godišnje ili češće u slučaju:

9.1.1.1 uvođenja novih tehnologija za udaljeni pristup

9.1.1.2 značajnog proširenja rada na daljinu (npr. inicijative hibridne radne snage)

9.1.1.3 pojave novih prijetnji, ranjivosti ili incidenata povezanih s udaljenim okruženjima

9.1.1.4 promjena relevantnog pravnog ili regulatornog okvira

9.2 Vlasništvo i postupak pregleda

9.2.1 Vlasnik politike je CISO. Pregled se mora koordinirati sa sljedećim funkcijama:

9.2.1.1 IT operacije i arhitektura

9.2.1.2 HR i upravljanje objektima (za operativne učinke i učinke na radni prostor)

9.2.1.3 službenik za zaštitu podataka (za privatnost i prekogranične kontrole podataka)

9.2.2 Ažuriranja politike moraju biti:

9.2.2.1 odobrena od strane Upravljačkog odbora ISMS-a

9.2.2.2 priopćena svom pogođenom osoblju i izvođačima

9.2.2.3 uključena u materijale za uvođenje u posao i obnovljeno osposobljavanje

9.3 Upravljanje dokumentom i distribucija

9.3.1 Politika mora sadržavati oznaku verzije, datum stupanja na snagu i povijest izmjena.

9.3.2 Prethodne verzije moraju se čuvati u skladu s Politikom upravljanja dokumentima (P14).

9.3.3 Revidirane verzije moraju zahtijevati obveznu ponovnu potvrdu upoznatosti za korisnike koji ispunjavaju uvjete za rad na daljinu.

10. Povezane politike i upućivanja

10.1 Ova politika primjenjuje se zajedno sa sljedećim politikama:

10.1.1 P1 – Politika informacijske sigurnosti: uspostavlja osnovu za sigurno rukovanje imovinom, primjenjivu u svim radnim okruženjima, uključujući rad na daljinu.

10.1.2 P3 – Politika prihvatljive uporabe: uređuje primjerenu uporabu organizacijskih uređaja i sustava tijekom sesija rada na daljinu.

10.1.3 P4 – Politika kontrole pristupa: osigurava da ovlasti za udaljeni pristup slijede načelo najmanjih ovlasti i odgovarajuće mehanizme autentikacije.

10.1.4 P6 – Politika upravljanja rizicima: definira kako se rizici rada na daljinu utvrđuju, obrađuju i prate unutar ISMS-a.

10.1.5 P12 – Politika upravljanja imovinom: zahtijeva evidenciju imovine i upravljanje konfiguracijom za sve uređaje koji se upotrebljavaju na daljinu.

10.1.6 P22 – Politika zapisivanja i praćenja: osigurava da se udaljene sesije prate, revidiraju i čuvaju u skladu sa zahtjevima usklađenosti.

10.1.7 P14 – Politika zadržavanja i zbrinjavanja podataka: definira pravila rukovanja podacima relevantna za rad na daljinu, uključujući prijenosne medije i zbrinjavanje uređaja.

10.2 Ove politike zajedno osiguravaju da je rad na daljinu siguran, usklađen i provediv u svim funkcijama i zemljopisnim područjima.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodno priznatim okvirima za sigurnost, zaštitu podataka i upravljanje ICT rizicima kako bi se osigurale sigurne, sljedive i usklađene prakse rada na daljinu.

11.2 ISO/IEC 27001

11.2.1 Točka 6.1.3 – planiranje obrade rizika: ova politika doprinosi obradi rizika povezanih s udaljenim pristupom i distribuiranim radnim okruženjima.

11.2.2 Točka 8.1 – operativno planiranje i kontrola: zahtijeva provedbu kontrola za sustave kojima se pristupa izvan prostora organizacije.

11.2.3 Prilog A, kontrola 6.7 – rad na daljinu: ova politika u cijelosti obuhvaća zahtijevane kontrole informacijske sigurnosti kada osoblje radi izvan prostora organizacije, uključujući fizičke i logičke zaštitne mjere, upravljanje pristupom i praćenje aktivnosti korisnika.

11.3 ISO/IEC 27002:2022 – kontrola 6

11.3.1 Ova kontrola propisuje organizacijske i tehničke zaštitne mjere za rad na daljinu. Uključuje zahtjeve za sigurnost uređaja, metode pristupa, rukovanje podacima, zaštitne mjere okruženja i upravljanje trećim stranama, a svi se provode ovom politikom.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (udaljeni pristup): izravno je podržan VPN kontrolama, MFA-om, zapisivanjem sesija i odobravanjem udaljenog pristupa na temelju uloga.

11.4.2 AC-2 (upravljanje računima): uređuje prihvatljivost za pristup, dodjelu udaljenih ovlasti i deaktivaciju računa.

11.4.3 SC-12 do SC-13 (kriptografska zaštita, uspostava kriptografskih ključeva): provode se obveznom uporabom VPN-a i enkripcije cijelog diska za udaljene krajnje uređaje.

11.4.4 MP-5 (zaštita prijenosa medija) i PE-18 (lokacija sastavnica informacijskog sustava): smjernice za rad na daljinu zahtijevaju zaštitu prijenosa i fizičke zaštitne mjere u okruženjima izvan lokacije.

11.4.5 AU-2, AU-6: zapisivanje i praćenje udaljenih sesija podupiru zahtjeve za reviziju i odgovor na incidente.

11.5 GDPR EU (2016/679)

11.5.1 Članak 32 – sigurnost obrade: ova politika osigurava kontrole sigurnosti udaljenog pristupa, enkripcije i zapisivanja potrebne za zaštitu osobnih podataka kojima se pristupa ili koji se obrađuju na daljinu.

11.5.2 Članak 5(1)(f): osigurava da su osobni podaci kojima se pristupa izvan lokacije zaštićeni od neovlaštene ili nezakonite obrade i slučajnog gubitka.

11.5.3 Uvodna izjava 39: naglašava ograničenje pristupa, cjelovitost i povjerljivost, osobito kada uređaji napuštaju sigurne prostore.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Članak 21(2)(a, b, d): zahtijeva da udaljeni pristup bude zaštićen kao dio okvira upravljanja ICT rizicima organizacije. Ova politika ispunjava zahtjev za sigurnosnim mjerama koje obuhvaćaju kontrolu pristupa, sigurnost podataka i organizacijske politike za udaljena okruženja.

11.6.2 Članak 21(3): potiče sigurnosnu osviještenost i poštivanje politike među osobljem koje radi izvan središnjih prostora.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Članak 5 – upravljanje i okvir unutarnjih kontrola: ova politika podupire očekivanja kontrole ICT rizika u svim operativnim scenarijima, uključujući hibridne i udaljene modele rada.

11.7.2 Članak 8 – okvir upravljanja ICT rizicima: rizici udaljenog pristupa utvrđuju se, ublažavaju i uređuju putem tehničkih i organizacijskih kontrola propisanih ovom politikom.

11.7.3 Članak 9 – aranžmani za razmjenu informacija: štiti od curenja informacija pri radu na daljinu unutar mreža digitalne operativne otpornosti.

11.8 COBIT 2019

11.8.1 DSS01 – upravljane operacije: ova politika podupire siguran kontinuitet poslovnih operacija neovisno o fizičkoj lokaciji.

11.8.2 BAI06 – upravljane IT promjene i BAI09 – upravljana imovina: osiguravaju da se uređaji za rad na daljinu prate, sigurno konfiguriraju i tretiraju kao kritična imovina.

11.8.3 APO13 – upravljana sigurnost: promiče definiran okvir upravljanja sigurnošću za udaljena okruženja.

11.8.4 MEA03 – pratiti, vrednovati i ocjenjivati usklađenost: uspostavlja zahtjev da aktivnosti rada na daljinu moraju biti evidentirane, pregledane i revidirane.