					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P07S					Naziv dokumenta: **Politika uvođenja u rad i prestanka radnog odnosa**							
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/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.2, 7	Zahtjevi za sigurnost ljudskih resursa i podizanje svijesti
ISO/IEC 27002:2022	Kontrole 6.2, 6.5	Sigurnosne prakse za uvođenje u rad i prestanak radnog odnosa
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Prestanak angažmana osoblja; životni ciklus korisničkih računa; planiranje
EU NIS2	Članak 21(2)(h)	Sigurnost ljudskih resursa i životni ciklus pristupa
EU DORA	Članak 12	Kontrola pristupa i opoziv pristupa za IKT sustave
COBIT 2019	APO07, DSS01	Sigurnost osoblja, kontrole logičkog i fizičkog pristupa
EU GDPR	Članak 32	Sigurnost osobnih podataka tijekom zaposlenja

1. Svrha

1.1 Ova politika definira postupak za uvođenje novih zaposlenika ili ugovornih izvršitelja u rad te sigurno uklanjanje pristupa kada osobe napuštaju organizaciju ili mijenjaju uloge.

1.2 Ova politika osigurava da se prava pristupa dodjeljuju u skladu s načelom najmanjih privilegija, da je sva imovina evidentirana te da se ključne aktivnosti, kao što su deaktivacija sustava i oporavak podataka, izvršavaju pravodobno.

1.3 Ova politika podupire usklađenost, operativni integritet i zaštitu podataka kroz strukturirane aktivnosti uvođenja u rad i prestanka radnog odnosa koje se mogu dokumentirati i revidirati.

2. Opseg

2.1 Ova politika primjenjuje se na:

2.1.1 sve stalne i privremene zaposlenike

2.1.2 ugovorne izvršitelje, konzultante i vježbenike

2.1.3 vanjske pružatelje usluga koji imaju sustavni ili fizički pristup

2.2 Ova politika obuhvaća:

2.2.1 uvođenje u rad: otvaranje korisničkih računa, dodjelu pristupa i izdavanje opreme

2.2.2 izlazni proces: uklanjanje pristupa, povrat imovine organizacije i sigurno zatvaranje digitalnih identiteta

2.2.3 interne promjene uloga koje zahtijevaju ponovnu konfiguraciju pristupa ili preraspodjelu imovine

2.3 Ova politika primjenjuje se na sve uređaje, platforme i lokacije koje se koriste za službene poslovne funkcije.

3. Ciljevi

3.1 Osigurati da novo osoblje dobije pristup i resurse na temelju provjerenih uloga i odgovornosti.

3.2 Potvrditi da se korisnicima koji odlaze do kraja njihova posljednjeg radnog dana u potpunosti ukida pristup sustavima i objektima.

3.3 Spriječiti postojanje napuštenih korisničkih računa i nevraćene imovine, koji predstavljaju sigurnosni rizik.

3.4 Održavati dokumentirane zapise o aktivnostima uvođenja u rad, premještaja i izlaznog procesa.

3.5 Osigurati odgovornost primjenom kontrolnih lista i međufunkcionalnom koordinacijom uloga.

4. Uloge i odgovornosti

4.1 Direktor

4.1.1 Odobrava pristup za uloge s visokim privilegijama i nadzire program uvođenja u rad i prestanka radnog odnosa.

4.1.2 Osigurava da su iznimke obrazložene te da se poduzimaju korektivne radnje kada se postupci ne poštuju.

4.2 Voditelj ureda / Ljudski resursi (HR)

4.2.1 Pokreće uvođenje novih zaposlenika u rad i obavještava IT o odlascima.

4.2.2 Osigurava dovršetak pravne dokumentacije (npr. NDA) i potvrde o upoznatosti s politikom.

4.2.3 Održava kontrolne liste za uvođenje u rad i izlazni proces te prati usklađenost s politikom.

[... 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

9.1.1 Ovu politiku moraju najmanje jednom godišnje pregledati Direktor i voditelji HR-a/IT-a.

9.2 Okidači za raniji pregled

9.2.1 Ažuriranja se moraju provesti ako:

9.2.1.1 se uvedu novi HR ili IT sustavi

9.2.1.2 dođe do promjene vanjskog pružatelja IT usluga ili pružatelja upravljanih HR usluga

9.2.1.3 sigurnosne revizije otkriju manjkavosti u postupcima

9.2.1.4 se promijene regulatorne obveze (npr. ažuriranja GDPR-a)

9.2.1.5 nastupi kritičan neuspjeh izlaznog procesa ili sigurnosni incident

9.3 Upravljanje verzijama i odobrenje

9.3.1 Svaka verzija ove politike mora sadržavati:

9.3.1.1 broj verzije i datum

9.3.1.2 sažetak promjena

9.3.1.3 odobrenje Direktora

9.3.1.4 arhivirane prethodne verzije koje se čuvaju najmanje tri godine

9.4 Komunikacija i potvrda upoznatosti

9.4.1 Sve osoblje odgovorno za uvođenje u rad ili prestanak radnog odnosa mora biti obaviješteno o svim ažuriranjima politike. Godišnja osvježavanja svijesti ili obnovno osposobljavanje su obvezni.

10. Povezane politike i poveznice

10.1 Ova politika podupire sljedeće dokumente i poduprta je njima:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: osigurava odgovornost u postupcima pristupa i uvođenja u rad

10.1.2 P4S – Politika kontrole pristupa: uspostavlja tehničku provedbu dodjele pristupa na temelju uloga i deaktivacije

10.1.3 P6S – Politika upravljanja rizicima: procjenjuje rizike koji proizlaze iz neuspjeha kontrola uvođenja u rad i prestanka radnog odnosa

10.1.4 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: propisuje zahtjeve za upoznavanje osoblja tijekom uvođenja u rad

10.1.5 P30S – Politika odgovora na incidente: tretira propust u ukidanju prava pristupa ili krađu imovine kao sigurnosne incidente

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.2 – uspostavlja zahtjeve za sigurnost ljudskih resursa

11.1.2 Točka 7.2 – propisuje osposobljavanje za podizanje svijesti za novo osoblje

11.2 ISO/IEC 27002

11.2.1 Kontrole 6.2 i 6.5 – detaljno uređuju sigurnosne prakse uvođenja u rad i prestanka radnog odnosa

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – postupci prestanka angažmana osoblja, uključujući deaktivaciju pristupa

11.3.2 AC-2 – osigurava upravljanje životnim ciklusom korisničkih računa za pristup

11.3.3 PL-4 – zahtijeva planiranje prijelaza osoblja

11.4 EU GDPR

11.4.1 Članak 32 – osigurava odgovarajuću sigurnost tijekom i nakon zaposlenja, osobito za pristup osobnim podacima

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(h) – zahtijeva sigurnost ljudskih resursa i kontrole životnog ciklusa pristupa

11.6 Uredba EU DORA

11.6.1 Članak 12 – zahtijeva da regulirani financijski subjekti kontroliraju pristup osoblja IKT sustavima, uključujući postupke opoziva pristupa

11.7 COBIT 2019

11.7.1 APO07 – Upravljanje ljudskim resursima: uspostavlja zahtjeve sigurnosti tijekom životnog ciklusa osoblja

11.7.2 DSS01 – Upravljanje operacijama: obuhvaća kontrolu logičkog i fizičkog pristupa tijekom prijelaza u radnom odnosu