					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P07					Naziv dokumenta: **Politika uvođenja u posao 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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 7.2, točka 6	Osposobljenost osoblja, sigurna integracija te provedba odgovornosti pri prestanku radnog odnosa ili promjeni radnog statusa.
ISO/IEC 27002:2022	Kontrole 6.2, 6.5, 5	Uvođenje u posao, pristup i kontrole životnog ciklusa osoblja.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Promjena radnog statusa i prestanak angažmana osoblja, načelo najmanjih privilegija, revizijsko bilježenje i upravljanje pristupom tijekom i nakon promjena statusa osoblja.
GDPR EU	Članci 5(1)(f), 25, 32; uvodna izjava 39	Ograničavanje pristupa, povjerljivost, zaštita i primjerene kontrole za osobne podatke osoblja.
Direktiva EU NIS2	Članak 21(2)(b, c, d)	Mjere sigurnosti osoblja i operativne sigurnosti; ublažavanje insajderskih prijetnji; procesi životnog ciklusa.
Uredba EU DORA	Članci 5, 8, 9	Upravljanje, unutarnje ICT kontrole, ICT rizik i upravljanje incidentima tijekom promjene statusa osoblja.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Ljudski resursi, upravljanje znanjem, sigurnost i usklađenost pri uvođenju u posao i prestanku radnog odnosa.

1. Svrha

1.1 Ovom se politikom uspostavljaju standardizirani postupci za upravljanje uvođenjem u posao, internim premještajima i prestankom radnog odnosa za sve vrste korisnika.

1.2 Njome se osigurava pravodobna i sigurna dodjela pristupnih prava i ukidanje pristupnih prava za fizički i logički pristup, uz provedbu zahtjeva povjerljivosti, odgovornosti te povrata i provjere imovine.

1.3 Ova politika ublažava rizike povezane s neovlaštenim pristupom, curenjem podataka i nevraćenom imovinom ugradnjom kontrola uvođenja u posao i prestanka radnog odnosa u procese ljudskih resursa (HR), IT-a i sigurnosti.

1.4 Ova politika podupire kontrolu 6.5 Dodatka A norme ISO/IEC 27001:2022 osiguravajući da se obveze sigurnosti osoblja provode tijekom i nakon zaposlenja ili angažmana.

2. Opseg

2.1 Ova se politika primjenjuje na sve zaposlenike, ugovorne izvođače, konzultante, dobavljače i druge treće strane kojima je odobren pristup sustavima, mrežama, objektima ili podacima organizacije.

2.2 Ova politika uređuje cjelokupan životni ciklus:

2.2.1 uvođenje u posao (zapošljavanje, ugovaranje ili privremeni angažman)

2.2.2 interni premještaji ili promjene uloge

2.2.3 izlazni proces (ostavka, umirovljenje, prestanak radnog odnosa, istek ugovora)

2.3 Ova politika obuhvaća:

2.3.1 logički pristup (sustavi, aplikacije, oblak, VPN)

2.3.2 fizički pristup (iskaznice, ključevi, sustavi ulaska u zgradu)

2.3.3 dodijeljenu imovinu (prijenosna računala, telefoni, tokeni, vjerodajnice)

2.3.4 potvrdu upoznatosti s politikom i obveze povjerljivosti

2.4 Svi odjeli (HR, IT, objekti, sigurnost i uprava) odgovorni su za izvršavanje svoje uloge u radnim tokovima uvođenja u posao i izlaznog procesa.

3. Ciljevi

3.1 Osigurati da se pristup odobrava svom osoblju tek nakon ispunjenja sigurnosnih, obrazovnih i ugovornih preduvjeta.

3.2 Opozvati pristupna prava i vratiti imovinu organizacije odmah po promjeni uloge ili prestanku radnog odnosa.

3.3 Očuvati povjerljivost, cjelovitost i dostupnost imovine organizacije tijekom promjena statusa osoblja.

3.4 Poduprijeti revizijsku sljedivost i pravnu dokazivost potpunim zapisima o događajima uvođenja u posao i prestanka radnog odnosa.

3.5 Smanjiti izloženost insajderskim prijetnjama provjerom i dokumentiranjem svih događaja pristupa povezanih s osobljem.

3.6 Uskladiti životni ciklus osoblja organizacije sa sigurnosnim praksama temeljenima na riziku i regulatornim zahtjevima.

4. Uloge i odgovornosti

4.1 Izvršni menadžment

4.1.1 Odobrava ovu politiku i dodjeljuje ovlasti i resurse za procese uvođenja u posao, izlaznog procesa i kontrole pristupa.

4.1.2 Osigurava da promjene statusa osoblja ne izlože organizaciju neprihvatljivom sigurnosnom ili pravnom riziku.

4.2 Ljudski resursi (HR)

4.2.1 Pokreću radne tokove uvođenja u posao i postupka prestanka radnog odnosa za zaposlenike te obavještavaju relevantne odjele o promjenama.

4.2.2 Osiguravaju da su sigurnosne provjere, ugovori, sporazumi o povjerljivosti i potvrde upoznatosti s politikama dovršeni prije odobravanja pristupa.

4.2.3 Obavještavaju IT i upravljanje objektima o odlasku osoblja u skladu sa SLA-om za obavješćivanje.

4.2.4 Koordiniraju s pravnim poslovima provedbu obveza nakon prestanka radnog odnosa (npr. odredbe o neotkrivanju podataka).

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

9. Pregled i ažuriranje zahtjeva

9.1 Učestalost pregleda politike

9.1.1 Ova politika mora se pregledati:

9.1.1.1 jednom godišnje, ili

9.1.1.2 nakon svakog značajnog incidenta koji uključuje zlouporabu pristupa, gubitak imovine ili neuspjeh postupka

9.1.1.3 pri provedbi značajnih promjena HR-a ili IAM platforme

9.1.1.4 nakon regulatornih ili pravnih izmjena koje utječu na podatke o osoblju ili povezane obveze

9.2 Postupak pregleda i vlasništvo

9.2.1 Voditelj ISMS-a i direktor HR-a koordiniraju pregled, uz doprinos IT sigurnosti, pravnih poslova i funkcije usklađenosti.

9.2.2 Sve promjene moraju odobriti izvršni menadžment i Upravljački odbor ISMS-a.

9.2.3 Revidirane verzije moraju se ponovno distribuirati pogođenim odjelima i osoblju radi ponovne potvrde upoznatosti.

9.3 Upravljanje dokumentom i zadržavanje

9.3.1 Ova politika mora uključivati:

9.3.2 upravljanje verzijama, povijest promjena i datum stupanja na snagu

9.3.3 odgovornog vlasnika i pregledavatelja

9.3.4 klasifikaciju politike i zapis o odobrenju

9.3.5 Zastarjele verzije moraju se arhivirati najmanje 3 godine u skladu s Politikom upravljanja dokumentima.

10. Povezane politike i poveznice

10.1.1 Ova je politika izravno povezana sa sljedećim politikama:

10.1.2 P1 – Politika informacijske sigurnosti: Uspostavlja sigurnosne ciljeve organizacije, uključujući upravljanje pristupom osoblja.

10.1.3 P4 – Politika kontrole pristupa: Utvrđuje operativne zahtjeve za dodjelu i opoziv pristupa sustavima i fizičkog pristupa na temelju okidača uvođenja u posao i prestanka radnog odnosa.

10.1.4 P3 – Politika prihvatljive uporabe: Zahtijeva potvrdu upoznatosti tijekom uvođenja u posao i podupire provedbu nakon prestanka radnog odnosa.

10.1.5 P6 – Politika upravljanja rizicima: Osigurava da se rizici pristupa korisnika i promjene statusa vrednuju i ublažavaju u skladu s načelima ISMS-a.

10.1.6 P11 – Politika upravljanja korisničkim računima i privilegijama: Uređuje tehničke kontrole za dodjelu i ukidanje pristupa kao potporu ovoj politici.

10.2 Ove politike čine integrirani sustav kontrola za sigurno i odgovorno upravljanje događajima u životnom ciklusu osoblja.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodno priznatim okvirima za sigurnost, privatnost i upravljanje IT-om kako bi se osiguralo da su procesi uvođenja u posao i prestanka radnog odnosa sigurni, sljedivi i usklađeni sa zakonskim i organizacijskim zahtjevima.

11.2 ISO/IEC 27001:

11.2.1 Točka 7.2 – Osposobljenost i točka 6.2 – ciljevi informacijske sigurnosti: Ova politika podupire uspostavu osposobljenosti osoblja i sigurnu integraciju osoba u uloge koje utječu na ciljeve ISMS-a.

11.2.2 Kontrola 6.5 Dodatka A – Odgovornosti nakon prestanka radnog odnosa ili promjene zaposlenja: Ova politika u cijelosti provodi kontrole nad preostalim pravima pristupa, skrbništvom nad podacima i ugovornim obvezama po odlasku.

11.2.3 Kontrola 5.9 Dodatka A – Provjera i 6.2 – Uvjeti zaposlenja: Postupci uvođenja u posao uključuju provjeru prethodne pozadine i mehanizme potvrde upoznatosti s politikama u skladu s tim točkama.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (prestanak angažmana osoblja) i PS-5 (premještaj osoblja): Ova politika provodi strukturirano uklanjanje ili izmjenu pristupnih prava, fizičkih iskaznica i imovine.

11.3.2 AC-2 (upravljanje računima) i AC-6 (načelo najmanjih privilegija): Odredbe osiguravaju da je pristup usklađen s ulogom i da se pravodobno opoziva kada više nije potreban.

11.3.3 IA-4 (upravljanje identifikatorima) i IA-5 (upravljanje autentifikatorima): Podupire sigurno upravljanje vjerodajnicama tijekom i nakon promjena statusa osoblja.

11.3.4 CM-5 (ograničenja pristupa za promjene): Sprječava neovlaštene promjene nakon prestanka radnog odnosa opozivom povišenih prava pristupa.

11.3.5 AU-2 i AU-6: bilježenje i sljedivost događaja pristupa dodatno se osnažuju integracijom IAM-a i revizijskog traga.

11.4 GDPR EU (2016/679):

11.4.1 Članak 5(1)(f): Štiti osobne podatke od neovlaštenog pristupa, što se u ovoj politici provodi opozivom korisničkog pristupa tijekom izlaznog procesa.

11.4.2 Članak 32: Propisuje odgovarajuće tehničke i organizacijske kontrole za zaštitu osobnih podataka tijekom životnog ciklusa zaposlenja.

11.4.3 Članak 25 – zaštita podataka ugrađena u dizajn: Osigurava da uvođenje u posao i prestanak radnog odnosa uključuju minimizaciju podataka, zadržavanje i zakonite kontrole pristupa.

11.4.4 Uvodna izjava 39: Naglašava ograničavanje pristupa i povjerljivost, što je podržano strukturom ove politike.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Članak 21(2)(b, c, d): Zahtijeva sigurnosne mjere za osoblje i operativnu sigurnost radi kontrole pristupa, ublažavanja insajderskih prijetnji i procesa životnog ciklusa, što je sve obuhvaćeno ovom politikom.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Članak 5 – upravljanje i unutarnje kontrole: Ova politika podupire unutarnje upravljanje ICT-om povezano s ljudskim rizikom i upravljanjem pristupom.

11.6.2 Članak 8 – upravljanje ICT rizikom: Primjenjuje kontrole na promjene statusa osoblja koje bi mogle izložiti kritičnu imovinu ili regulirana okruženja.

11.6.3 Članak 9 – klasifikacija i upravljanje incidentima: Osigurava da se povrede povezane s prestankom radnog odnosa mogu prijaviti i ublažiti pravilnim ukidanjem pristupa i postupanjem s imovinom.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Definira uloge, odgovornosti i aktivnosti životnog ciklusa za uvođenje u posao i prestanak radnog odnosa usklađene s ciljevima upravljanja.

11.7.2 BAI08 – Knowledge Management: Osnažuje dokumentiranje postupaka, zadržavanje znanja i prijenos kontrola na kraju zaposlenja.

11.7.3 DSS05 – Managed Security Services: Provodi deaktivaciju korisnika, kontrolu imovine i odgovornost tijekom prijelaza uloga.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Osigurava da se kontrole uvođenja u posao i izlaznog procesa ocjenjuju tijekom unutarnjih i vanjskih revizija.