					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P07S					Naslov dokumenta: **Politika uvajanja in prenehanja sodelovanja**							
Različica: 1.0		Datum začetka veljavnosti: 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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzuli 6.2, 7	Zahteve glede kadrovske varnosti in ozaveščanja
ISO/IEC 27002:2022	Kontroli 6.2, 6.5	Varnostne prakse pri uvajanju in prenehanju sodelovanja
NIST SP 800-53 Rev. 5	PS-4, AC-2, PL-4	Prenehanje sodelovanja osebja, upravljanje življenjskega cikla računov, načrtovanje
Direktiva EU NIS2	Člen 21(2)(h)	Kadrovska varnost in življenjski cikel dostopov
Uredba EU DORA	Člen 12	Kontrole dostopa in preklic dostopa za sisteme IKT
COBIT 2019	APO07, DSS01	Varnost osebja, kontrole logičnega in fizičnega dostopa
Uredba EU GDPR	Člen 32	Varnost osebnih podatkov med zaposlitvijo

1. Namen

1.1 Ta politika določa postopek uvajanja novih zaposlenih ali pogodbenih izvajalcev ter varnega odvzema dostopa, ko posamezniki zapustijo organizacijo ali zamenjajo vlogo.

1.2 Zagotavlja, da se dostop dodeljuje v skladu z načelom najmanjših privilegijev, da so vsa sredstva evidentirana ter da se ključna dejanja, kot sta deaktivacija sistemov in prenos podatkov, izvedejo pravočasno.

1.3 Ta politika podpira skladnost, operativno celovitost in varstvo podatkov s strukturiranimi dejavnostmi uvajanja in prenehanja sodelovanja, ki so preverljive v reviziji.

2. Področje uporabe

2.1 Ta politika velja za:

2.1.1 vse redno in začasno zaposlene;

2.1.2 pogodbene izvajalce, svetovalce in praktikante;

2.1.3 zunanje ponudnike storitev s sistemskim ali fizičnim dostopom.

2.2 Zajema:

2.2.1 uvajanje: vzpostavitev uporabniških računov, dodelitev dostopa, izdajo opreme;

2.2.2 prenehanje sodelovanja: odstranitev dostopa, vračilo sredstev podjetja in varno ukinitev digitalnih identitet;

2.2.3 notranje spremembe vlog, ki zahtevajo ponovno nastavitev dostopa ali prerazporeditev sredstev.

2.3 Velja za vse naprave, platforme in lokacije, ki se uporabljajo za uradne poslovne funkcije.

3. Cilji

3.1 Zagotoviti, da novo osebje prejme dostop in vire na podlagi preverjenih vlog in odgovornosti.

3.2 Zagotoviti, da se uporabnikom, ki odhajajo, do konca zadnjega delovnega dne v celoti odvzame dostop do sistemov in prostorov.

3.3 Preprečiti osirotele račune in nevračena sredstva, ki predstavljajo varnostno tveganje.

3.4 Vzdrževati dokumentirane evidence o uvajanju, premestitvah in prenehanju sodelovanja.

3.5 Krepiti odgovornost z uporabo kontrolnih seznamov in medfunkcijskim usklajevanjem vlog.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Odobrava dostop za uporabnike z visokimi privilegiji in nadzira program uvajanja in prenehanja sodelovanja.

4.1.2 Zagotavlja, da so izjeme utemeljene in da se sprejmejo korektivni ukrepi, kadar se postopki ne upoštevajo.

4.2 Vodja pisarne / kadrovska služba (HR)

4.2.1 Začne postopek uvajanja novih zaposlenih in obvesti IT o odhodih.

4.2.2 Zagotavlja dokončanje pravne dokumentacije (npr. pogodbe o nerazkrivanju informacij) in potrditev varnostnih politik.

4.2.3 Vzdržuje kontrolne sezname za uvajanje in prenehanje sodelovanja ter spremlja skladnost s politiko.

[... 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

9.1.1 To politiko morajo najmanj enkrat letno pregledati generalni direktor ter vodji HR in IT.

9.2 Sprožilci predčasnega pregleda

9.2.1 Posodobitve se morajo izvesti, če:

9.2.1.1 se uvedejo novi sistemi HR ali IT;

9.2.1.2 se zamenja zunanji ponudnik IT-storitev ali zunanja kadrovska storitev;

9.2.1.3 varnostne presoje razkrijejo vrzeli v postopkih;

9.2.1.4 se spremenijo regulativne obveznosti (npr. posodobitve GDPR);

9.2.1.5 pride do kritične napake v postopku prenehanja sodelovanja ali do kršitve.

9.3 Upravljanje različic in odobritev

9.3.1 Vsaka različica te politike mora vključevati:

9.3.1.1 številko različice in datum;

9.3.1.2 povzetek sprememb;

9.3.1.3 odobritev generalnega direktorja;

9.3.1.4 arhivirane prejšnje različice, ki se hranijo najmanj tri leta.

9.4 Komunikacija in potrditev

9.4.1 Vse osebje, odgovorno za uvajanje ali prenehanje sodelovanja, mora biti obveščeno o vseh posodobitvah politike. Letne seznanitve za ozaveščanje ali osvežitvene seznanitve so obvezne.

10. Povezane politike in povezave

10.1 Ta politika podpira naslednje politike in je z njimi povezana:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: zagotavlja odgovornost v postopkih dostopa in uvajanja;

10.1.2 P4S – Politika upravljanja dostopa: določa tehnično uveljavitev dodeljevanja in deaktivacije na podlagi vlog;

10.1.3 P6S – Politika upravljanja tveganj: ocenjuje tveganja, ki izhajajo iz odpovedi kontrol pri uvajanju in prenehanju sodelovanja;

10.1.4 P8S – Politika ozaveščanja in usposabljanja na področju informacijske varnosti: določa zahteve glede uvodnega usposabljanja osebja med uvajanjem;

10.1.5 P30S – Politika upravljanja incidentov informacijske varnosti: obravnava neizveden odvzem dostopa ali krajo sredstev kot varnostna incidenta.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.2 – določa zahteve glede kadrovske varnosti.

11.1.2 Klavzula 7.2 – določa obveznost usposabljanja za ozaveščanje novih članov osebja.

11.2 ISO/IEC 27002

11.2.1 Kontroli 6.2 in 6.5 – podrobneje določata varnostne prakse pri uvajanju in prenehanju zaposlitve.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – postopki prenehanja sodelovanja osebja, vključno z deaktivacijo dostopa.

11.3.2 AC-2 – zagotavlja upravljanje življenjskega cikla računov za uporabniški dostop.

11.3.3 PL-4 – zahteva načrtovanje prehodov osebja.

11.4 Uredba EU GDPR

11.4.1 Člen 32 – zahteva ustrezno varnost med zaposlitvijo in po njej, zlasti pri dostopu do osebnih podatkov.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(h) – zahteva kadrovsko varnost in kontrole življenjskega cikla dostopov.

11.6 Uredba EU DORA

11.6.1 Člen 12 – zahteva, da regulirani finančni subjekti nadzorujejo dostop osebja do sistemov IKT, vključno s postopki preklica.

11.7 COBIT 2019

11.7.1 APO07 – upravljanje človeških virov: določa zahteve glede varnosti v celotnem življenjskem ciklu osebja.

11.7.2 DSS01 – upravljanje operacij: zajema nadzor logičnega in fizičnega dostopa med kadrovskimi prehodi.