					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P07					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	Clause 7.2, Clause 6	Kompetence osebja, varna vključitev v delo ter izvajanje odgovornosti ob prenehanju ali spremembi delovnega razmerja.
ISO/IEC 27002:2022	Controls 6.2, 6.5, 5	Kontrole za uvajanje, dostop in življenjski cikel osebja.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Prehodi in prenehanje sodelovanja osebja, načelo najmanjših privilegijev, revizijsko beleženje ter upravljanje dostopa med spremembami statusa osebja in po njih.
EU GDPR	Articles 5(1)(f), 25, 32; Recital 39	Omejevanje dostopa, zaupnost, zaščita in ustrezne kontrole za osebne podatke zaposlenih in drugih posameznikov.
EU NIS2	Article 21(2)(b, c, d)	Kadrovski in operativni varnostni ukrepi, zmanjševanje notranjih groženj ter procesi življenjskega cikla.
EU DORA	Articles 5, 8, 9	Upravljanje, notranje kontrole IKT, tveganja IKT in upravljanje incidentov med prehodi osebja.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Človeški viri, upravljanje znanja, varnost in skladnost pri uvajanju in prenehanju sodelovanja.

1. Namen

1.1 Ta politika določa standardizirane postopke za upravljanje uvajanja, notranjih premestitev in prenehanja sodelovanja za vse vrste uporabnikov.

1.2 Zagotavlja pravočasno in varno dodeljevanje ter odvzem pravic fizičnega in logičnega dostopa ter hkrati uveljavlja zaupnost, odgovornost in vračilo sredstev.

1.3 Ta politika zmanjšuje tveganja, povezana z nepooblaščenim dostopom, uhajanjem podatkov in nevrnjenimi sredstvi, tako da vključuje kontrole uvajanja in prenehanja v procese človeških virov, IT in varnosti.

1.4 Podpira ISO/IEC 27001:2022, Prilogo A, kontrolo 6.5, tako da zagotavlja izvajanje obveznosti varnosti osebja med zaposlitvijo ali sodelovanjem ter po njunem prenehanju.

2. Področje uporabe

2.1 Ta politika velja za vse zaposlene, pogodbene izvajalce, svetovalce, dobavitelje in druge tretje osebe, ki imajo odobren dostop do sistemov, omrežij, prostorov ali podatkov organizacije.

2.2 Ureja celoten življenjski cikel:

2.2.1 uvajanja (zaposlitev, pogodbeno sodelovanje ali začasna angažiranost),

2.2.2 notranjih premestitev ali sprememb vlog,

2.2.3 postopka izstopa (odpoved, upokojitev, prenehanje, iztek pogodbe).

2.3 Politika zajema:

2.3.1 logični dostop (sistemi, aplikacije, oblak, VPN),

2.3.2 fizični dostop (identifikacijske kartice, ključi, sistemi za vstop v objekte),

2.3.3 dodeljena sredstva (prenosniki, telefoni, žetoni, poverilnice),

2.3.4 potrditve politik in obveznosti glede zaupnosti.

2.4 Za izvajanje svojih vlog v delovnih tokovih uvajanja in postopka izstopa so odgovorni vsi oddelki (človeški viri, IT, upravljanje objektov, varnost in vodstvo).

3. Cilji

3.1 Zagotoviti, da se vsem članom osebja dostop odobri šele po izpolnitvi varnostnih, izobraževalnih in pogodbenih predpogojev.

3.2 Ob spremembi vloge ali prenehanju sodelovanja nemudoma preklicati pravice dostopa in zagotoviti vračilo sredstev organizacije.

3.3 Ohraniti zaupnost, celovitost in razpoložljivost (CIA) sredstev organizacije med prehodi osebja.

3.4 Podpreti preverljivost in pravno zaščito s popolnimi evidencami o dogodkih uvajanja in prenehanja sodelovanja.

3.5 Zmanjšati izpostavljenost notranjim grožnjam s preverjanjem in dokumentiranjem vseh dogodkov dostopa, povezanih z osebjem.

3.6 Uskladiti življenjski cikel osebja organizacije z varnostnimi praksami, temelječimi na tveganjih, in regulativnimi zahtevami.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri to politiko ter dodeli pooblastila in vire za procese uvajanja, postopka izstopa in upravljanja dostopa.

4.1.2 Zagotovi, da prehodi osebja v organizaciji ne povzročajo nesorazmernih varnostnih ali pravnih tveganj.

4.2 Človeški viri

4.2.1 Za zaposlene sprožijo delovne tokove uvajanja in prenehanja sodelovanja ter o spremembah obvestijo pristojne oddelke.

4.2.2 Zagotovijo, da so preverjanje preteklosti, pogodbe, dogovor o nerazkrivanju informacij in potrditve politik zaključeni pred odobritvijo dostopa.

4.2.3 V skladu z dogovorjenimi ravnmi storitev za obveščanje obvestijo IT in upravljanje objektov o odhodih zaposlenih.

4.2.4 Sodelujejo s pravno službo pri uveljavljanju obveznosti po prenehanju zaposlitve ali sodelovanja (npr. klavzul o nerazkrivanju).

[... 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 Pogostost pregleda politike

9.1.1 To politiko je treba pregledati:

9.1.1.1 letno ali

9.1.1.2 po vsakem bistvenem incidentu, ki vključuje zlorabo dostopa, izgubo sredstev ali neuspeh postopka,

9.1.1.3 ob uvedbi večjih sprememb platform človeških virov ali IAM,

9.1.1.4 ob regulativnih ali pravnih spremembah, ki vplivajo na osebne podatke ali obveznosti.

9.2 Postopek pregleda in lastništvo

9.2.1 Vodja ISMS in direktor kadrovske funkcije usklajujeta pregled ob prispevku IT, informacijske varnosti, pravne službe in funkcije skladnosti.

9.2.2 Vse spremembe morata odobriti najvišje vodstvo in usmerjevalni odbor ISMS.

9.2.3 Revidirane različice morajo biti ponovno posredovane zadevnim oddelkom in osebju v ponovno potrditev.

9.3 Nadzor dokumenta in hramba

9.3.1 Ta politika mora vključevati:

9.3.2 upravljanje različic, evidenco sprememb in datum začetka veljavnosti,

9.3.3 določenega lastnika in pregledovalca(-e),

9.3.4 klasifikacijo politike in evidenco odobritve.

9.3.5 Zastarele različice se morajo arhivirati najmanj 3 leta v skladu s Politiko upravljanja dokumentov.

10. Povezane politike in povezave

10.1.1 Ta politika je neposredno povezana z:

10.1.2 P1 – Politika informacijske varnosti: določa varnostne cilje organizacije, vključno z upravljanjem dostopa osebja.

10.1.3 P4 – Politika nadzora dostopa: določa operativne zahteve za dodeljevanje in preklic sistemskega ter fizičnega dostopa na podlagi sprožilcev uvajanja in prenehanja sodelovanja.

10.1.4 P3 – Politika sprejemljive uporabe (AUP): zahteva potrditev ob uvajanju in podpira izvrševanje ob prenehanju sodelovanja.

10.1.5 P6 – Politika upravljanja tveganj: zagotavlja, da se tveganja uporabniškega dostopa in prehodov ocenjujejo ter zmanjšujejo v skladu z načeli ISMS.

10.1.6 P11 – Politika upravljanja uporabniških računov in privilegijev: ureja tehnične kontrole za dodeljevanje in odvzem dostopa v podporo tej politiki.

10.2 Te politike skupaj tvorijo integriran sistem kontrol za varno in odgovorno upravljanje dogodkov v življenjskem ciklu osebja.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi okviri informacijske varnosti, zasebnosti in upravljanja IT, da zagotovi, da so postopki uvajanja in prenehanja sodelovanja varni, sledljivi in skladni s pravnimi ter organizacijskimi zahtevami.

11.2 ISO/IEC 27001:

11.2.1 Klavzula 7.2 – Kompetence in klavzula 6.2 – Cilji informacijske varnosti: Ta politika podpira vzpostavitev kompetenc osebja in varno vključitev posameznikov v vloge, v katerih vplivajo na cilje ISMS.

11.2.2 Priloga A, kontrola 6.5 – Odgovornosti po prenehanju ali spremembi zaposlitve: Ta politika v celoti uveljavlja kontrole nad preostalimi pravicami dostopa, skrbništvom nad podatki in pogodbenimi obveznostmi ob odhodu.

11.2.3 Priloga A, kontrola 5.9 – Preverjanje in 6.2 – Pogoji zaposlitve: Postopki uvajanja vključujejo mehanizme preverjanja preteklosti in potrditve politike v skladu s temi določbami.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Prenehanje sodelovanja osebja) in PS-5 (Premestitev osebja): Ta politika uveljavlja strukturirano odstranitev ali spremembo pravic dostopa, fizičnih kartic in sredstev.

11.3.2 AC-2 (Upravljanje računov) in AC-6 (Načelo najmanjših privilegijev): Določbe zagotavljajo, da je dostop usklajen z vlogo in pravočasno preklican, ko ni več potreben.

11.3.3 IA-4 (Upravljanje identifikatorjev) in IA-5 (Upravljanje avtentikatorjev): Podpira varno upravljanje poverilnic med spremembami statusa osebja in po njih.

11.3.4 CM-5 (Omejitve dostopa za spremembe): Preprečuje nepooblaščene spremembe po prenehanju sodelovanja s preklicem povišanih pravic dostopa.

11.3.5 AU-2 in AU-6: Beleženje in sledljivost dogodkov dostopa sta okrepljena z integracijo IAM in revizijsko sledjo.

11.4 Uredba EU GDPR (2016/679):

11.4.1 Člen 5(1)(f): Varuje osebne podatke pred nepooblaščenim dostopom, kar se v tej politiki zagotavlja s preklicem uporabniškega dostopa med postopkom izstopa.

11.4.2 Člen 32: Zahteva ustrezne tehnične in organizacijske kontrole za zavarovanje osebnih podatkov skozi celoten življenjski cikel zaposlitve ali sodelovanja.

11.4.3 Člen 25 – Vgrajeno in privzeto varstvo podatkov: Zagotavlja, da uvajanje in prenehanje sodelovanja vključujeta minimizacijo podatkov, hrambo in zakonite kontrole dostopa.

11.4.4 Uvodna izjava 39: Poudarja omejevanje dostopa in zaupnost, kar podpira struktura te politike.

11.5 Direktiva EU NIS2 (2022/2555):

11.5.1 Člen 21(2)(b, c, d): Zahteva kadrovske in operativne varnostne ukrepe za obravnavo nadzora dostopa, zmanjševanja notranjih groženj in procesov življenjskega cikla, kar je vključeno v to politiko.

11.6 Uredba EU DORA (2022/2554):

11.6.1 Člen 5 – Upravljanje in notranja kontrola: Ta politika podpira notranje upravljanje IKT, povezano s človeškimi tveganji in upravljanjem dostopa.

11.6.2 Člen 8 – Obvladovanje tveganj IKT: Uporablja kontrole za prehode osebja, ki bi lahko izpostavili kritična sredstva ali regulirana okolja.

11.6.3 Člen 9 – Razvrščanje in upravljanje incidentov: Zagotavlja, da so kršitve, povezane s prenehanjem sodelovanja, prijavljive in zmanjšane z ustreznim odvzemom dostopa ter ravnanjem s sredstvi.

11.7 COBIT 2019:

11.7.1 APO07 – Upravljani človeški viri: Določa vloge, odgovornosti in dejavnosti življenjskega cikla za uvajanje in prenehanje sodelovanja, usklajene s cilji upravljanja.

11.7.2 BAI08 – Upravljanje znanja: Krepi dokumentiranje postopkov, hrambo znanja in prenos kontrol ob koncu zaposlitve.

11.7.3 DSS05 – Upravljane varnostne storitve: Uveljavlja deaktivacijo uporabnikov, nadzor nad sredstvi in odgovornost med prehodi vlog.

11.7.4 MEA03 – Spremljanje, vrednotenje in presoja skladnosti: Zagotavlja, da se kontrole uvajanja in postopka izstopa presojajo v okviru notranjih in zunanjih revizij.