					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P11S					Naslov dokumenta: **Politika upravljanja uporabniških računov in privilegijev**							
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 5.3, 8	Vloge, odgovornosti ter operativno načrtovanje in nadzor za upravljanje uporabniškega dostopa
ISO/IEC 27002:2022	Kontrola 8	Kontrole za dodeljevanje, pregled in odvzem povišanih privilegijev
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Ustvarjanje računov, spremljanje, načelo najmanjših privilegijev in ločevanje dolžnosti (SoD)
Direktiva EU NIS2	Člen 21(2)(d)	Upravljanje uporabniškega dostopa za bistvene in pomembne subjekte
Uredba EU DORA	Člen 9(2)(b)	Nadzor privilegiranega dostopa pri finančnih subjektih
COBIT 2019	DSS05.03, DSS05.04	Dodeljevanje dostopa, ukinitev in periodični pregled uporabniškega dostopa
Uredba EU GDPR	Člen 32	Ustrezne kontrole dostopa za varstvo osebnih podatkov

1. Namen

1.1 Ta politika določa pravila za upravljanje uporabniških računov in pravic dostopa na varen, dosleden in sledljiv način. Zagotavlja, da imajo dostop do sistemov in podatkov samo pooblaščeni uporabniki ter da je dostop ustrezen glede na njihovo vlogo in odgovornosti.

1.2 Učinkovito upravljanje računov in privilegijev je bistveno za preprečevanje nepooblaščenega dostopa, zmanjševanje notranjih groženj in zagotavljanje skladnosti z zahtevami standarda ISO/IEC 27001, Uredbe EU GDPR in drugih predpisov.

1.3 Ta politika organizaciji omogoča dodelitev lastništva in odgovornosti za uporabo računov, spremljanje in revidiranje povišanih privilegijev ter varno onemogočanje ali preklic dostopa, ko ta ni več potreben.

1.4 Politika varuje tudi poslovanje pred operativnimi napakami ali neprimerno uporabo, ki je posledica prekomernega ali nenadzorovanega dostopa, ter pomaga zmanjševati tveganje nenamernega razkritja podatkov, neprimerne uporabe privilegijev ali regulatorne neskladnosti.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse zaposlene, praktikante, pogodbene izvajalce in uporabnike tretjih oseb z dostopom do informacijskih sistemov organizacije;

2.1.2 vse sisteme, naprave, storitve in platforme, ki jih upravlja organizacija ali se upravljajo v njenem imenu, vključno z oblačnimi platformami, infrastrukturo na lokaciji in orodji tretjih oseb.

2.2 Zajema vse vrste uporabniških računov, vključno z:

2.2.1 imenovanimi uporabniškimi računi (npr. e-poštni računi, sistemske prijave);

2.2.2 administratorskimi in sistemskimi računi;

2.2.3 začasnimi, gostujočimi računi ali poverilnicami za dostop tretjih oseb;

2.2.4 storitvenimi računi, ki jih uporabljajo aplikacije ali avtomatizirani sistemi.

2.3 Politika velja skozi celoten življenjski cikel računa – od ustvarjanja in odobritve do sprememb, spremljanja in deaktivacije. To vključuje začetno dodelitev dostopa med uvajanjem, preglede pravic dostopa ob spremembah vlog in preklic v okviru postopka izstopa.

3. Cilji

3.1 Vsem uporabnikom sistemov dodeliti enolične in sledljive uporabniške identitete ter zagotoviti odgovornost in odpravo odvisnosti od skupnih poverilnic.

3.2 Uveljaviti načelo najmanjših privilegijev ter zagotoviti, da se uporabnikom dodeli le najmanjši obseg dostopa, potreben za opravljanje njihovih nalog.

3.3 Preprečiti nepooblaščen dostop do občutljivih sistemov ali podatkov z jasno dokumentiranimi postopki odobritve in pregleda.

3.4 Zagotoviti pravočasno deaktivacijo uporabniških računov, ko ti niso več potrebni, na primer ob prenehanju zaposlitve, zaključku pogodbenega razmerja ali spremembi vloge.

3.5 Z dokumentiranjem vseh sprememb računov, odobritev in periodičnih pregledov vzdrževati varno okolje, pripravljeno za revizijo.

3.6 Zagotoviti, da je povišanje privilegijev strogo nadzorovano, neodvisno odobreno in revizijsko zabeleženo ter da se povišani dostop nemudoma prekliče, ko ni več potreben.

4. Vloge in odgovornosti

4.1 Generalni direktor

4.1.1 Nosi splošno odgovornost za uveljavljanje te politike.

4.1.2 Zagotavlja, da so prakse upravljanja računov usklajene z zahtevami za certificiranje po ISO/IEC 27001 in ustreznimi pravnimi obveznostmi (npr. Uredba EU GDPR).

4.1.3 O vsakem nepooblaščenem dostopu, varnostnem incidentu ali kršitvi politike, povezani z uporabniškimi računi, mora biti obveščen nemudoma.

4.1.4 Nadzoruje preglede politike, revizije in izvršilne ukrepe.

4.2 Vodja IT ali zunanji ponudnik IT-storitev

4.2.1 Odgovoren je za tehnično uvedbo kontrol računov in privilegijev v sistemih, ki jih uporablja organizacija.

4.2.2 Uporabniške račune sme dodeliti, spremeniti in deaktivirati izključno na podlagi dokumentiranih odobritev.

4.2.3 Zagotoviti mora ustrezno zahtevnost gesel, časovno omejitev neaktivnosti zaslona, večfaktorsko avtentikacijo (MFA), kjer je na voljo, ter sistemsko beleženje dnevnikov.

4.2.4 Vzdrževati mora varne evidence vseh odobritev dostopa, lastništva računov, povišanj privilegijev in preklicev.

4.2.5 Spremljati mora nepooblaščene ali osirotele račune ter o neskladjih poročati generalnemu direktorju.

[... 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 To politiko morata generalni direktor in vodja IT pregledati najmanj enkrat letno, da se zagotovi skladnost z:

9.1.1 veljavnimi kontrolami in smernicami ISO/IEC 27001:2022,

9.1.2 regulatornimi posodobitvami (npr. Uredba EU GDPR, Uredba EU DORA, Direktiva EU NIS2),

9.1.3 spremembami sistemov, storitev ali poslovne strukture.

9.2 Preglede je treba izvesti tudi po:

9.2.1 pomembnih varnostnih incidentih ali ugotovitvah presoje,

9.2.2 večjih spremembah informacijskih sistemov ali arhitekture računov,

9.2.3 uvedbi novih platform, ki zahtevajo integracijo nadzora dostopa.

9.3 Vse spremembe mora odobriti generalni direktor in jih je treba jasno sporočiti zadevnemu osebju.

10. Povezane politike in povezave

10.1 P2S – Politika vlog in odgovornosti upravljanja: določa odgovornosti in pooblastila odločanja za odobritve dostopa in nadzor.

10.2 P4S – Politika nadzora dostopa: ureja izvajanje nadzora dostopa na ravni sistemov in metode avtentikacije.

10.3 P7S – Politika uvajanja in prenehanja: zagotavlja, da sta ustvarjanje in odstranitev računov vključena v kadrovsko vodene spremembe osebja.

10.4 P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: uporabnike usposablja glede varne uporabe računov in pričakovanj glede uporabe.

10.5 P30S – Politika odzivanja na incidente: določa ukrepe, ki jih je treba izvesti, če neprimerna uporaba računa povzroči varnostni incident ali nepooblaščeno razkritje.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 5.3 zahteva, da so vloge in odgovornosti za informacijsko varnost jasno dodeljene in uveljavljene.

11.1.2 Klavzula 8.1 zahteva, da operativno načrtovanje in nadzor vključujeta upravljanje uporabniškega dostopa.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.2 podrobneje določa tehnične in postopkovne kontrole za dodeljevanje, pregled in odvzem povišanih privilegijev.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2 zahteva ustvarjanje računov, spremljanje in preklic na podlagi opredeljenih vlog in procesov.

11.3.2 AC-5 obravnava ločevanje dolžnosti (SoD) za preprečevanje nasprotja interesov ali zlorabe privilegijev.

11.3.3 AC-6 zahteva uporabo načela najmanjših privilegijev za vse pravice dostopa.

11.4 Uredba EU GDPR

11.4.1 Člen 32 zahteva ustrezne kontrole dostopa za zaščito osebnih podatkov pred nepooblaščenim dostopom ali spremembo.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(d) zahteva upravljanje uporabniškega dostopa kot del temeljnih varnostnih kontrol za bistvene in pomembne subjekte.

11.6 Uredba EU DORA

11.6.1 Člen 9(2)(b) zahteva, da finančni subjekti uvedejo kontrole dostopa, ki omejujejo in spremljajo privilegirane pravice.

11.7 COBIT 2019

11.7.1 DSS05.03 določa dodeljevanje dostopa in ukinitev uporabniškega dostopa kot del upravljanja IT.

11.7.2 DSS05.04 zahteva stalni pregled in usklajevanje uporabniškega dostopa z organizacijskimi vlogami.