					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P11S					Naziv dokumenta: **Politika upravljanja korisničkim računima i privilegijama**							
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**

Usklađenost sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.3, 8	Uloge, odgovornosti te operativno planiranje i kontrola za upravljanje korisničkim pristupom
ISO/IEC 27002:2022	Kontrola 8	Kontrole za dodjelu, pregled i uklanjanje povišenih privilegija
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Uspostava računa, praćenje, načelo najmanjih privilegija i razdvajanje dužnosti (SoD)
EU NIS2	Članak 21(2)(d)	Upravljanje korisničkim pristupom za ključne i važne subjekte
EU DORA	Članak 9(2)(b)	Kontrola privilegiranog pristupa u financijskim subjektima
COBIT 2019	DSS05.03, DSS05.04	Dodjela prava pristupa, ukidanje prava pristupa i periodični pregled korisničkog pristupa
GDPR EU	Članak 32	Odgovarajuće kontrole pristupa za zaštitu osobnih podataka

1. Svrha

1.1 Ova politika uspostavlja pravila za upravljanje korisničkim računima i pravima pristupa na siguran, dosljedan i sljediv način. Njome se osigurava da samo ovlašteni korisnici imaju pristup sustavima i podacima te da je pristup primjeren njihovoj ulozi i odgovornostima.

1.2 Učinkovito upravljanje računima i privilegijama ključno je za sprječavanje neovlaštenog pristupa, smanjenje insajderskih prijetnji i osiguravanje usklađenosti s normom ISO/IEC 27001, GDPR-om i drugim regulatornim zahtjevima.

1.3 Ova politika omogućuje organizaciji dodjelu vlasništva i odgovornosti za korištenje računa, praćenje i reviziju eskalacije privilegija te sigurno onemogućavanje ili ukidanje prava pristupa kada više nisu potrebna.

1.4 Ova politika također štiti poslovne operacije od operativnih pogrešaka ili zlouporabe uzrokovane prekomjernim ili nenadziranim pristupom te pomaže smanjiti rizik od slučajnog otkrivanja podataka, zlouporabe privilegija ili regulatorne neusklađenosti.

2. Opseg

2.1 Ova se politika primjenjuje na:

2.1.1 sve zaposlenike, vježbenike, ugovorne izvođače i korisnike trećih strana koji imaju pristup IT sustavima organizacije

2.1.2 sve sustave, uređaje, usluge i platforme kojima upravlja organizacija ili kojima se upravlja u njezino ime, uključujući platforme u oblaku, lokalnu infrastrukturu i alate trećih strana

2.2 Obuhvaća sve vrste korisničkih računa, uključujući:

2.2.1 imenovane korisničke račune (npr. račune e-pošte, prijave u sustav)

2.2.2 administratorske račune i račune na razini sustava

2.2.3 privremene, gostujuće ili pristupne vjerodajnice trećih strana

2.2.4 servisne račune koje koriste aplikacije ili automatizirani sustavi

2.3 Politika se primjenjuje tijekom cijelog životnog ciklusa računa — od uspostave i odobrenja do izmjene, praćenja i deaktivacije. To uključuje početnu dodjelu prava pristupa tijekom uvođenja u posao, preglede pristupa tijekom promjena uloge te ukidanje prava pristupa tijekom izlaznog procesa.

3. Ciljevi

3.1 Dodijeliti jedinstvene korisničke identitete, sljedive za sve korisnike sustava, kako bi se osigurala odgovornost i uklonilo oslanjanje na zajedničke vjerodajnice.

3.2 Primjenjivati načelo najmanjih privilegija, tako da se korisnicima dodjeljuje samo minimalna razina pristupa potrebna za obavljanje njihovih dužnosti.

3.3 Spriječiti neovlašteni pristup osjetljivim sustavima ili podacima putem jasno dokumentiranih postupaka odobravanja i pregleda.

3.4 Osigurati pravodobnu deaktivaciju korisničkih računa kada više nisu potrebni, primjerice pri prestanku radnog odnosa, završetku ugovora ili promjeni uloge.

3.5 Održavati sigurno okruženje i spremnost za reviziju dokumentiranjem svih promjena računa, odobrenja i periodičnih pregleda.

3.6 Osigurati da je eskalacija privilegija strogo kontrolirana, neovisno odobrena i evidentirana te da se povišeni pristup ukida bez odgode kada više nije potreban.

4. Uloge i odgovornosti

4.1 Glavni rukovoditelj (GM)

4.1.1 Snosi ukupnu odgovornost za provedbu ove politike.

4.1.2 Osigurava da su prakse upravljanja računima usklađene sa zahtjevima za certifikaciju prema ISO/IEC 27001 i relevantnim pravnim obvezama (npr. GDPR).

4.1.3 Mora biti bez odgode obaviješten o svakom neovlaštenom pristupu, sigurnosnom incidentu ili kršenju politike povezanom s korisničkim računima.

4.1.4 Nadzire preglede politike, revizije i mjere provedbe.

4.2 IT voditelj ili vanjski pružatelj IT usluga

4.2.1 Odgovoran je za tehničku provedbu kontrola računa i privilegija u sustavima koje organizacija koristi.

4.2.2 Mora dodijeliti, izmijeniti i deaktivirati korisničke račune isključivo na temelju dokumentiranih odobrenja.

4.2.3 Mora provoditi zahtjeve za složenost lozinki, automatsko zaključavanje zaslona nakon isteka vremena neaktivnosti, višefaktorsku autentifikaciju (MFA), gdje je dostupna, i revizijsko bilježenje.

4.2.4 Mora voditi sigurne evidencije o svim odobrenjima pristupa, vlasništvu nad računima, eskalacijama privilegija i ukidanjima prava pristupa.

4.2.5 Mora pratiti neovlaštene ili napuštene korisničke račune i prijaviti odstupanja GM-u.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledati najmanje jednom godišnje od strane GM-a i IT voditelja kako bi se osigurala usklađenost sa:

9.1.1 važećim kontrolama i smjernicama norme ISO/IEC 27001:2022

9.1.2 regulatornim ažuriranjima (npr. GDPR, DORA, NIS2)

9.1.3 promjenama u sustavima, uslugama ili poslovnoj strukturi

9.2 Pregledi se moraju provoditi i nakon:

9.2.1 značajnih sigurnosnih incidenata ili nalaza revizije

9.2.2 velikih promjena u IT sustavima ili arhitekturi računa

9.2.3 uvođenja novih platformi koje zahtijevaju integraciju kontrole pristupa

9.3 Sve promjene mora odobriti GM i one moraju biti jasno priopćene zahvaćenom osoblju.

10. Povezane politike i poveznice

10.1 P2S – Politika uloga i odgovornosti u upravljanju: Uspostavlja odgovornosti i ovlasti za odobravanje pristupa i nadzor.

10.2 P4S – Politika kontrole pristupa: Uređuje provedbu kontrole pristupa na razini sustava i metode autentifikacije.

10.3 P7S – Politika uvođenja u posao i prestanka radnog odnosa: Osigurava da su uspostava i uklanjanje računa uključeni u promjene osoblja kojima upravlja HR.

10.4 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: Osposobljava korisnike za sigurne prakse korištenja računa i očekivani način uporabe.

10.5 P30S – Politika odgovora na incidente: Definira radnje koje treba poduzeti ako zlouporaba računa dovede do sigurnosnog incidenta ili neovlaštenog otkrivanja podataka.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 5.3: Zahtijeva da uloge i odgovornosti za informacijsku sigurnost budu jasno dodijeljene i provedene.

11.1.2 Točka 8.1: Operativno planiranje i kontrola moraju uključivati upravljanje korisničkim pristupom.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.2: Opisuje tehničke i proceduralne kontrole za dodjelu, pregled i uklanjanje povišenih privilegija.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Zahtijeva uspostavu, praćenje i ukidanje računa na temelju definiranih uloga i procesa.

11.3.2 AC-5: Uređuje razdvajanje dužnosti (SoD) radi sprječavanja sukoba ili zlouporabe privilegija.

11.3.3 AC-6: Propisuje primjenu načela najmanjih privilegija na sva prava pristupa.

11.4 GDPR EU

11.4.1 Članak 32: Zahtijeva odgovarajuće kontrole pristupa radi zaštite osobnih podataka od neovlaštenog pristupa ili izmjene.

11.5 EU NIS

11.5.1 Članak 21(2)(d): Propisuje upravljanje korisničkim pristupom kao dio temeljnih sigurnosnih kontrola za ključne i važne subjekte.

11.6 EU DORA

11.6.1 Članak 9(2)(b): Zahtijeva da financijski subjekti provedu kontrole pristupa koje ograničavaju i prate privilegirana prava.

11.7 COBIT 2019

11.7.1 DSS05.03: Propisuje dodjelu prava pristupa i ukidanje prava pristupa korisnika kao dio IT upravljanja.

11.7.2 DSS05.04: Zahtijeva kontinuirani pregled i usklađivanje korisničkog pristupa s organizacijskim ulogama.