					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P11					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	Točka 6.1.3, točka 8	-
ISO/IEC 27002:2022	Kontrole 5.15-5	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
GDPR EU	Članci 5(1)(f), 32; uvodna izjava 39	-
Direktiva EU NIS2	Članci 21(2)(a, d), 21(3)	-
Uredba EU DORA	Članci 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Svrha

1 Ova politika utvrđuje obvezne kontrole za upravljanje korisničkim računima i privilegijama u svim informacijskim sustavima i uslugama. Njome se osigurava da se pristup resursima organizacije dodjeljuje na temelju provjerenog identiteta, poslovne potrebe proizašle iz uloge te načela najmanjih privilegija i razdvajanja dužnosti (SoD).

1.1 Ova politika podupire opredijeljenost organizacije za informacijsku sigurnost uspostavom strukturiranih procesa za otvaranje korisničkih računa, dodjelu privilegija, praćenje uporabe i ukidanje prava pristupa, koji su primjereni za reviziju.

1.2 Ova politika ključna je za smanjenje rizika od neovlaštenog pristupa, zlouporabe privilegija, insajderskih prijetnji i neusklađenosti s primjenjivim regulatornim okvirima.

2. Opseg

2.1 Ova politika primjenjuje se na sve zaposlenike, ugovorne izvođače, pružatelje usluga trećih strana, konzultante i druge osobe kojima je odobren pristup IT resursima, aplikacijama ili podacima organizacije.

2.2 Ova politika uređuje sve sustave i okruženja u kojima se primjenjuju mehanizmi autentifikacije korisnika i kontrole pristupa, uključujući, ali ne ograničavajući se na:

2.2.1 poslovne aplikacije i baze podataka

2.2.2 platforme u oblaku i SaaS okruženja

2.2.3 operacijske sustave i administrativne konzole

2.2.4 alate za udaljeni pristup i VPN-ove

2.2.5 sustave za upravljanje identitetima i pristupom (IAM)

2.3 Ova politika obuhvaća standardne i povlaštene korisničke račune te uključuje kontrole nad:

2.3.1 otvaranjem, izmjenom i deaktivacijom računa

2.3.2 eskalacijom privilegija i delegiranjem

2.3.3 kontrolom sesija i praćenjem

2.3.4 metodama autentifikacije i upravljanjem vjerodajnicama

3. Ciljevi

3.1 Osigurati da su svi korisnički računi jednoznačno povezani s korisnikom, pravilno odobreni i dodijeljeni tek nakon formalne provjere potrebe za pristupom.

3.2 Primijeniti načelo najmanjih privilegija i spriječiti nepotreban ili prekomjeran pristup provedbom strogih kontrola nad dodjelom i uporabom povlaštenih računa.

3.3 Zahtijevati pravodobno ažuriranje statusa računa na temelju promjena zaposlenja ili uloge, uključujući trenutačnu deaktivaciju po prestanku radnog odnosa.

3.4 Omogućiti proaktivno otkrivanje i otklanjanje neaktivnih, zloupotrijebljenih ili neovlaštenih računa putem dnevničkih zapisa, pregleda i automatizacije.

3.5 Održavati usklađenost s normom ISO/IEC 27001:2022 i povezanim standardima te ispuniti obveze iz relevantnih pravnih i regulatornih okvira kao što su GDPR, NIS2, DORA i COBIT 2019.

4. Uloge i odgovornosti

4.1 Glavni službenik za informacijsku sigurnost (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu provedbu u cijeloj organizaciji.

4.1.2 Pregledava i odobrava sve formalne iznimke i slučajeve hitnog pristupa.

4.1.3 Izvještava o revizijskim nalazima povezanima s računima i eskalira rizike izvršnom rukovodstvu.

4.2 Voditelj kontrole pristupa / IT administrator

4.2.1 Održava i upravlja tehničkim kontrolama za upravljanje životnim ciklusom korisničkih računa.

4.2.2 Provodi dodjelu prava pristupa, ukidanje prava pristupa i aktivnosti upravljanja privilegijama na temelju odobrenog zahtjeva.

4.2.3 Vodi vjerodostojan registar svih korisničkih računa, njihova statusa i razina privilegija.

4.2.4 Podupire revizije i preglede usklađenosti dnevničkim zapisima i izvješćima o aktivnostima.

[... 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 pregledavati najmanje jednom godišnje ili pri značajnim promjenama u:

9.1.1 organizacijskoj strukturi ili poslovnim procesima

9.1.2 IT sustavima, platformama identiteta ili metodama pristupa

9.1.3 regulatornim ili ugovornim zahtjevima povezanima s upravljanjem identitetom i pristupom

9.2 Glavni službenik za informacijsku sigurnost (CISO), zajedno s Voditeljem kontrole pristupa, odgovoran je za pokretanje postupka pregleda i koordinaciju povratnih informacija dionika.

9.3 Izvanredni pregledi mogu se pokrenuti zbog:

9.3.1 sigurnosnih incidenata povezanih sa zlouporabom računa

9.3.2 revizijskih nalaza koji ukazuju na nedostatke u upravljanju životnim ciklusom računa

9.3.3 uvođenja novih alata za upravljanje identitetom ili upravljanje privilegiranim pristupom (PAM)

9.4 Ažuriranja ove politike moraju biti:

9.4.1 pod verzijskom kontrolom i evidentirana u repozitoriju dokumenata ISMS-a

9.4.2 priopćena svim relevantnim dionicima, uključujući voditelje odjela, IT operacije i HR

9.4.3 podržana ažuriranim materijalima za osposobljavanje i proceduralnim uputama

9.5 Sve promjene mora odobriti izvršno rukovodstvo ili Upravljački odbor za informacijsku sigurnost te moraju biti evidentirane za potrebe revizije.

10. Povezane politike i poveznice

10.1 Ova je politika operativno povezana sa sljedećim politikama unutar skupa politika ISMS-a i njima je podržana:

10.1.1 P4 Politika kontrole pristupa: Uspostavlja krovna načela i mehanizme kontrole pristupa, uključujući kontrole temeljene na pravilima i kontrolu pristupa temeljenu na ulogama (RBAC).

10.1.2 P7 Politika uvođenja u posao i prestanka radnog odnosa: Definira postupovne korake za otvaranje i ukidanje korisničkog pristupa usklađene s aktivnostima HR-a.

10.1.3 P8 Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: Jača odgovornosti korisnika za sigurnost računa i zaštitu vjerodajnica.

10.1.4 P13 Politika klasifikacije i označavanja podataka: Usmjerava razine pristupa na temelju klasifikacije podataka, osiguravajući da granice privilegija odgovaraju razinama osjetljivosti.

10.1.5 P22 Politika bilježenja i praćenja: Osigurava da se revizijski tragovi prikupljaju za sve aktivnosti povezane s računima i pregledavaju radi otkrivanja anomalija ili neovlaštene uporabe.

10.1.6 P30 Politika odgovora na incidente: Uređuje eskalaciju, ograničavanje i aktivnosti nakon incidenta u slučajevima zlouporabe privilegija ili neovlaštene aktivnosti računa.

10.2 Sve navedene politike zajedno provode usklađen, na riziku temeljen okvir upravljanja identitetima i pristupom u cijeloj organizaciji.

11. Referentni standardi i okviri

11.1 Ova je politika usklađena s globalno priznatim standardima kibernetičke sigurnosti i regulatornim okvirima koji zahtijevaju sigurno upravljanje identitetima, pristupom i privilegijama kao temeljnu sastavnicu informacijske sigurnosti organizacije.

11.2 ISO/IEC 27001:

11.2.1 Točka 6.1.3 zahtijeva da organizacije utvrde, vrednuju i obrađuju rizike informacijske sigurnosti, čime upravljanje pristupom i privilegijama postaje formalna kontrola temeljena na riziku, ugrađena u proces planiranja ISMS-a.

11.2.2 Točka 8.1 - Operativno planiranje i kontrola: Naglašava provedbu tehničkih i postupovnih zaštitnih mjera koje uređuju korisnički i povlašteni pristup.

11.3 ISO/IEC 27002:2022 - Kontrole 5.15 do 5:

11.3.1 Kontrola 5.15 - Upravljanje korisničkim pristupom: Podupire formalne procese za dodjelu računa, odobravanje pristupa i periodični pregled prava pristupa.

11.3.2 Kontrola 5.16 - Upravljanje identitetima: Uspostavlja jedinstvenost identiteta, kontrole životnog ciklusa i provedbu sigurne autentifikacije.

11.3.3 Kontrola 5.17 osigurava da su dodjela i uporaba povlaštenih prava pristupa strogo kontrolirane, sljedive i usklađene s načelom najmanjih privilegija tijekom cijelog životnog ciklusa korisničkog računa.

11.3.4 Kontrola 5.18 - Povlaštena prava pristupa: U potpunosti je obuhvaćena dodjelom privilegija temeljenom na ulogama, revizijom i zahtjevima za odobravanje povišenog pristupa.

11.4 Ove kontrole usmjeravaju strukturiranu provedbu registracije računa, odjave računa, razdvajanja privilegija i uporabe autentifikacijskih podataka. Politika provodi upravljanje životnim ciklusom identiteta, just-in-time pristup i praćenje povišenih sesija radi sprječavanja neovlaštene uporabe sustava.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Politika kontrole pristupa) i AC-2 (Upravljanje računima): Preslikani su kroz zahtjeve politike za odobravanje pristupa, mapiranje uloga i reviziju korisničkih računa.

11.5.2 AC-5 (Razdvajanje dužnosti) i AC-6 (Najmanje privilegije): Ispunjeni su ograničavanjem privilegija, usklađivanjem s radnim ulogama i dvostrukim odobrenjem za zadatke visokog rizika.

11.5.3 IA-2 do IA-5 (Identifikacija i autentifikacija): Provode se putem snažnih mehanizama autentifikacije, pravila životnog ciklusa vjerodajnica i zahtjeva za MFA.

11.5.4 AU-2, AU-12 (Revizijsko bilježenje i analiza): Obuhvaćeni su snimanjem sesija i praćenjem povlaštenih aktivnosti u osjetljivim okruženjima.

11.6 GDPR EU (2016/679):

11.6.1 Članak 32 - Sigurnost obrade: Zahtijeva kontrole pristupa i mehanizme provjere identiteta radi zaštite osobnih podataka. Ispunjava se obvezom odobravanja računa, pregleda privilegija i snažnih zaštitnih mjera autentifikacije.

11.6.2 Članak 5(1)(f) - Cjelovitost i povjerljivost: Osigurava da osobnim podacima pristupaju samo ovlašteni korisnici s legitimnim ulogama, što se dodatno osigurava primjenom upravljanja računima.

11.6.3 Uvodna izjava 39: Zahtijeva jasno ograničavanje pristupa i odgovornost — ova politika podupire potpunu sljedivost korisničkih identiteta i dodjele privilegija.

11.7 Direktiva EU NIS2 (2022/2555):

11.7.1 Članak 21(2)(a, d): Zahtijeva od subjekata provedbu politika upravljanja pristupom i sigurno postupanje s vjerodajnicama i povlaštenim sesijama, što je podržano kontrolama dodjele, praćenja i iznimki iz ove politike.

11.7.2 Članak 21(3): Promiče disciplinu pristupa i snažno osiguranje identiteta u kritičnim sektorima, što se ostvaruje primjenom jedinstvenih identifikatora, RBAC-a i vremenski ograničenog povišenog pristupa.

11.8 Uredba EU DORA (2022/2554):

11.8.1 Članak 5 - Upravljanje i kontrola IKT-a: Zahtijeva formalizirane procese za upravljanje IKT korisnicima, što je obuhvaćeno dokumentiranom dodjelom, deaktivacijom i postupanjem s iznimkama.

11.8.2 Članak 9 - Upravljanje IKT rizicima: Usmjerava organizacije da zaštite sustave ograničenjima pristupa i praćenjem, što se provodi putem MFA-a, bilježenja povlaštenog pristupa i centraliziranih pregleda.

11.9 COBIT 2019:

11.9.1 DSS01 - Upravljane operacije: Promiče provedbu standardiziranih operativnih kontrola, uključujući upravljanje životnim ciklusom korisničkih računa i dokumentiranje pristupa.

11.9.2 DSS05 - Upravljane sigurnosne usluge: Odražava sigurno administriranje korisničkih i sistemskih privilegija te podupire ublažavanje rizika kroz načelo najmanjih privilegija i provjeru revizijskog traga.

11.9.3 APO13 - Upravljana sigurnost: Zahtijeva upravljanje pristupom digitalnoj imovini, što se ispunjava formaliziranim praksama odobravanja računa i uloga uz obvezne periodične preglede.