					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P04					Naziv dokumenta: **Politika kontrole pristupa**							
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**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.15, 5.17, 5.18	Upravljanje logičkim i fizičkim pristupom
ISO/IEC 27002:2022	Kontrole 8.2, 8.3	Pristup temeljen na ulogama i upravljanje identitetima
NIST SP 800-53 Rev.5	AC-1 do AC-20, IA-1 do IA-8	Kontrole računa i pristupa, identitet i autentifikacija
GDPR EU	Članci 5(1)(f), 32(1)(b); uvodna izjava 39	Zaštita i minimizacija podataka
Direktiva EU NIS2	Članak 21(2)(c–e)	Kontrola pristupa, autentifikacija korisnika i zaštita imovine
Uredba EU DORA	Članci 6, 9(2)	IKT, pristup korisnika i snažne kontrole za treće strane
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Uvođenje u rad, operacije, praćenje i usklađenost

1. Svrha

1.1 Ova politika utvrđuje obvezna načela, odgovornosti i zahtjeve za kontrole upravljanja pristupom informacijskim sustavima, aplikacijama, fizičkim lokacijama i podatkovnoj imovini u cijeloj organizaciji.

1.2 Njome se osigurava da se pristup dodjeljuje na temelju poslovne potrebe, radne funkcije i profila rizika, uz primjenu načela najmanjih privilegija, načela nužnog poznavanja i razdvajanja dužnosti (SoD).

1.3 Ova politika podupire provedbu točke 5.15 norme ISO/IEC 27001:2022 i povezanih kontrola kojima se uređuju logički i fizički pristup, autentifikacija korisnika i upravljanje životnim ciklusom pristupa.

1.4 Ova politika čini temelj zaštite digitalnih i fizičkih resursa od neovlaštene uporabe, zlouporabe ili kompromitacije.

2. Opseg

2.1 Ova se politika primjenjuje na sve korisnike, sustave i lokacije unutar opsega ISMS-a, uključujući:

2.1.1 zaposlenike, ugovorne izvođače, dobavljače i privremeno osoblje

2.1.2 infrastrukturu u vlastitim prostorijama, sustave hostirane u oblaku i hibridna okruženja

2.1.3 svu organizacijsku imovinu — hardver, softver, podatke i zaštićena fizička područja

2.1.4 logički pristup (npr. sustavima, mrežama, aplikacijama i programskim sučeljima) i fizički pristup (npr. zgradama i podatkovnim centrima)

2.2 Uređuje pristup tijekom cijelog životnog ciklusa identiteta i interakcije s resursima, od uvođenja u rad i dodjele pristupnih prava do promjena uloga i izlaznog procesa.

2.3 Politika obuhvaća i korištenje vlastitih uređaja (BYOD) te udaljeni pristup, uz osiguravanje dosljednih kontrola neovisno o lokaciji i modelu vlasništva nad uređajem.

3. Ciljevi

3.1 Uspostaviti sigurnu kontrolu pristupa temeljenu na ulogama (RBAC) koja podupire operativni integritet i usklađenost s regulatornim zahtjevima.

3.2 Osigurati da se pristupna prava pravodobno odobravaju, prate i ukidaju.

3.3 Spriječiti neovlašteni pristup, eskalaciju sustavnih privilegija ili zadržavanje zastarjelih pristupnih prava.

3.4 Poduprijeti načela zero trust tako da se pristup prema zadanim postavkama odbija, osim ako nije izričito odobren i opravdan.

3.5 Osigurati revizorima i dionicima dokazivu razinu pouzdanosti putem automatiziranih pregleda pristupa i provedbe politike utemeljene na dokazima.

3.6 Ugraditi kontrolu pristupa u poslovne procese, događaje životnog ciklusa u području ljudskih resursa i tehničku arhitekturu.

4. Uloge i odgovornosti

4.1 Izvršni menadžment

4.1.1 Odobrava politiku kontrole pristupa te osigurava odgovarajući proračun i resurse za njezinu provedbu.

4.1.2 Tijekom preispitivanja uprave pregledava rizike povezane s kontrolom pristupa i dodjeljuje odgovornosti na strateškoj razini.

4.2 CISO / voditelj ISMS-a

4.2.1 Vlasnik je okvira kontrole pristupa i osigurava usklađenost s normom ISO/IEC 27001 i povezanim standardima.

4.2.2 Koordinira provedbu politike, testiranje kontrola, otklanjanje nedostataka te izvješćivanje o metrikama kontrole pristupa.

4.2.3 Nadzire modeliranje pristupa temeljeno na riziku i prati sustavne nedostatke kontrola.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Okidači i učestalost pregleda

9.1.1 Ova politika mora se pregledati:

9.1.1.1 jednom godišnje, ili

9.1.1.2 nakon velike promjene IT infrastrukture, regulatornih zahtjeva ili profila rizika

9.1.1.3 nakon incidenata koji otkriju slabosti u kontrolama pristupa

9.1.1.4 kada nastupe značajne promjene u tehnologijama autentifikacije ili platformama identiteta

9.2 Nadležnost i postupak pregleda

9.2.1 CISO ili imenovani voditelj ISMS-a upravlja ciklusom pregleda, uz uključivanje:

9.2.1.1 nalaza unutarnje revizije

9.2.1.2 rezultata i metrika pregleda pristupa

9.2.1.3 pravnih i regulatornih ažuriranja

9.2.1.4 promjena tehnoloških platformi

9.2.2 Sve izmjene mora odobriti izvršni menadžment i o njima obavijestiti sve dionike.

9.2.3 Od pogođenih korisnika može se zahtijevati da ponovno daju potvrdu upoznatosti s politikom nakon značajnih ažuriranja.

9.3 Upravljanje verzijama i dokumentacija

9.3.1 Glavna verzija mora biti pohranjena u repozitoriju dokumenata ISMS-a sa sljedećim metapodacima:

9.3.1.1 broj verzije i zapisnik promjena

9.3.1.2 datum stupanja na snagu i datum sljedećeg pregleda

9.3.1.3 vlasnik i ovlast za odobrenje

9.3.1.4 distribucija i zapisi o potvrdama upoznatosti

9.3.2 Zamijenjene verzije moraju se arhivirati i biti dostupne najmanje 3 godine.

10. Povezane politike i međusobne veze

10.1 Ova politika funkcionalno ovisi o sljedećim politikama i mora se tumačiti zajedno s njima:

10.1.1 P01 – Politika informacijske sigurnosti: definira opredijeljenost organizacije za sigurnost i očekivanja visoke razine u pogledu kontrole pristupa.

10.1.2 P03 – Politika prihvatljive uporabe: utvrđuje pravila ponašanja za pristup i odgovornost korisnika za odgovorno korištenje sustava.

10.1.3 P05 – Politika upravljanja promjenama: uređuje kako se promjene konfiguracija pristupa, uloga ili struktura grupa moraju provesti i sigurno testirati.

10.1.4 P07 – Politika uvođenja u rad i prestanka radnog odnosa: pokreće dodjelu i ukidanje pristupnih prava u skladu s događajima životnog ciklusa korisnika.

10.1.5 P11 – Politika upravljanja korisničkim računima i privilegijama: provodi kontrole na razini računa i nadopunjuje ovu politiku smjernicama za tehničku provedbu kontrole pristupa.

10.2 Zajedno, ove politike čine koherentan i provediv okvir za upravljanje pravima pristupa u svim poslovnim jedinicama i tehnologijama.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001:2022:

11.1.1 Točka 5.15 – kontrola pristupa: Ova politika ispunjava zahtjev za kontrolu pristupa informacijama i drugoj povezanoj imovini na temelju poslovnih zahtjeva i zahtjeva informacijske sigurnosti.

11.1.2 Točka 5.17 – upravljanje identitetom i točka 5.18 – informacije za autentifikaciju: provode se kroz dodjelu identiteta, mehanizme autentifikacije i dodjelu privilegija.

11.1.3 Kontrole Dodatka A 8.2 (Politika kontrole pristupa) i 8.3 (upravljanje identitetom): čine temelj ciljeva kontrola ove politike, uključujući pristup temeljen na ulogama, integraciju životnog ciklusa korisnika i zaštitu povlaštenog pristupa.

11.2 NIST SP 800-53 Rev.5:

11.2.1 Obitelj AC (AC-1 do AC-20): Ova politika podupire NIST-ove zahtjeve kontrole pristupa za fizičke i logičke sustave, uključujući definiranje politike (AC-1), upravljanje računima (AC-2) i razdvajanje dužnosti (AC-5).

11.2.2 Obitelj IA (IA-1 do IA-8): pruža smjernice za autentifikaciju identiteta, zaštitu vjerodajnica i MFA.

11.2.3 AU-2, AU-12: zahtjevi za bilježenje i reviziju koji se provode ovom politikom podupiru odgovornost korisnika i istragu incidenata.

11.2.4 PE-2 do PE-6: odnose se na ograničenja fizičkog pristupa, koja ova politika djelomično provodi putem kontrola iskaznica i ovlasti pristupa zgradama.

11.3 GDPR EU (2016/679):

11.3.1 Članak 5(1)(f): Osobni podaci moraju biti zaštićeni od neovlaštenog pristupa. Ova politika osigurava tehničku i proceduralnu provedbu tog načela.

11.3.2 Članak 32(1)(b): zahtijeva provedbu kontrola pristupa, pseudonimizacije i šifriranja radi sprječavanja neovlaštene obrade osobnih podataka.

11.3.3 Uvodna izjava 39: nalaže minimizaciju pristupa osobnim podacima, što se ovdje provodi kroz načelo najmanjih privilegija i zahtjeve za opravdanje pristupa.

11.4 Direktiva EU NIS2 (2022/2555):

11.4.1 Članak 21(2)(c–e): Ova politika omogućuje tehničke i organizacijske mjere za kontrolu pristupa, autentifikaciju korisnika i zaštitu imovine kod ključnih i važnih subjekata.

11.5 Uredba EU DORA (2022/2554):

11.5.1 Članak 6: zahtijeva politike upravljanja IKT rizicima koje izričito uključuju upravljanje pristupom korisnika i kontrole životnog ciklusa identiteta. Ova politika ispunjava taj zahtjev za financijski sektor i sektor IKT usluga.

11.5.2 Članak 9(2): Ova politika podupire provedbu snažnih kontrola pristupa kao dijela upravljanja IKT uslugama trećih strana i unutar grupe.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: provodi kontrole uvođenja u rad i izlaznog procesa radi podrške upravljanju pravima pristupa.

11.6.2 BAI03 – Managed Solutions Identification and Build: ugrađuje zahtjeve kontrole pristupa u projektiranje sustava i procese promjena.

11.6.3 DSS01 – Managed Operations i DSS05 – Managed Security Services: uređuju provedbu ograničenja logičkog pristupa i praćenje kršenja.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: podupire mehanizme revizije i osiguranja za provjeru djelotvornosti kontrole pristupa.