					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P04S					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 propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 5	
ISO/IEC 27002:2022	Kontrole: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev.5	AC-1 do AC-5	
GDPR EU	Članak 32	
Direktiva EU NIS2	Članak 21(2)(b)	
Uredba EU DORA	Članak 9	
COBIT 2019	APO07, DSS01	

1. Svrha

1.1. Ova politika definira način na koji organizacija upravlja pristupom sustavima, podacima i objektima kako bi se osiguralo da informacijama mogu pristupati samo ovlaštene osobe, na temelju poslovne potrebe.

1.2. Ovom politikom uspostavljaju se jasna pravila za dodjelu pristupnih prava, njihove izmjene, praćenje i ukidanje korisničkog pristupa radi smanjenja rizika od neovlaštenog pristupa i podrške usklađenosti s primjenjivim zakonima i standardima.

1.3. Ova politika provodi načelo najmanjih privilegija, prema kojem pristup mora biti ograničen na minimum potreban za obavljanje radnih zadataka.

2. Područje primjene

2.1. Ova politika primjenjuje se na sve osobe koje koriste ili upravljaju pristupom informacijskim sustavima, mrežama, podacima ili objektima organizacije, uključujući:

2.1.1. zaposlenike

2.1.2. ugovorne izvođače

2.1.3. privremene radnike

2.1.4. vanjske pružatelje IT usluga

2.2. Obuhvaća pristup:

2.2.1. aplikacijama organizacije, dijeljenim datotekama i bazama podataka

2.2.2. sustavima elektroničke pošte, VPN-u i udaljenom pristupu

2.2.3. uslugama u oblaku koje se koriste u poslovne svrhe

2.2.4. fizičkom pristupu sigurnim područjima, kao što su uredi ili poslužiteljske sobe

2.3. Ova se politika primjenjuje na svim uređajima koje je izdala organizacija ili na odobrenim BYOD uređajima, kao i na svim platformama i lokacijama.

3. Ciljevi

3.1. Osigurati da se prava pristupa dodjeljuju isključivo nakon formalnog odobrenja, na temelju uloge i poslovnog opravdanja.

3.2. Spriječiti neovlašten pristup ili prekomjerne ovlasti nad osjetljivim podacima, sustavima ili infrastrukturom.

3.3. Definirati jasne postupke za dodjelu, izmjenu i ukidanje korisničkog pristupa.

3.4. Zahtijevati redovite preglede pristupa te automatizirano ili ručno vođenje revizijskih zapisa kao podršku revizijama.

3.5. Podržati tehničku provedbu ograničenja pristupa putem odgovarajuće konfiguracije i praćenja.

4. Uloge i odgovornosti

4.1. Glavni direktor

4.1.1. Odobrava ovu politiku i osigurava dostupnost resursa za uspostavu učinkovitih kontrola pristupa.

4.1.2. Odobrava iznimke i pregledava godišnje revizije pristupa.

4.2. Voditelj IT-a / vanjski pružatelj IT usluga

4.2.1. Upravlja dodjelom, izmjenom i ukidanjem korisničkih računa.

4.2.2. Održava registar kontrole pristupa sa svim aktivnostima dodjele, izmjene i uklanjanja pristupa.

4.2.3. Uspostavlja kontrolu pristupa temeljenu na ulogama (RBAC) i provodi snažnu autentifikaciju, primjerice MFA.

4.2.4. Pregledava dnevnike pristupa radi otkrivanja sumnjivih aktivnosti i prijavljuje uočene nepravilnosti glavnom direktoru.

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

9. Pregled i ažuriranje zahtjeva

9.1. Godišnji pregled politike

9.1.1. Voditelj IT-a mora pregledati ovu politiku najmanje jednom godišnje. Svaka promjena u pravnom, tehničkom ili organizacijskom kontekstu mora dovesti do njezina neposrednog ažuriranja.

9.2. Okidači za pregled

9.2.1. Politika se mora pregledati i ako nastupi bilo koji od sljedećih događaja:

9.2.2. veće promjene sustava ili migracije u oblak

9.2.3. promjene uloga ili organizacijske strukture

9.2.4. sigurnosni incident koji uključuje neovlašten pristup

9.2.5. regulatorne promjene, primjerice ažuriranja GDPR-a, NIS2 ili DORA-e

9.3. Dokumentiranje i priopćavanje promjena

9.3.1. Izmjene moraju biti evidentirane s poviješću verzija, odobrenjem glavnog direktora i priopćene svom obuhvaćenom osoblju.

9.4. Dostupnost i osposobljavanje

9.4.1. Ova politika mora biti dostupna svim zaposlenicima, a odgovarajuće osposobljavanje mora se provoditi kao dio uvođenja u posao i jednom godišnje nakon toga.

10. Povezane politike i poveznice

10.1. Ova se politika treba primjenjivati usklađeno sa sljedećim SME politikama radi potpune provedbe sigurnih praksi upravljanja pristupom:

10.1.1. P3S – Politika prihvatljive uporabe: osigurava da korisnici razumiju prihvatljivo ponašanje pri korištenju dodijeljenog pristupa.

10.1.2. P5S – Politika upravljanja promjenama: osigurava da su prava pristupa usklađena s odobrenim promjenama sustava.

10.1.3. P7S – Politika uvođenja u posao i prestanka radnog odnosa: definira točke pokretanja za dodjelu i ukidanje pristupnih prava korisnika.

10.1.4. P17S – Politika zaštite podataka i privatnosti: osigurava da su kontrole pristupa usklađene sa zaštitnim mjerama za osobne podatke.

10.1.5. P30S – Politika odgovora na incidente: definira kako se upravlja incidentima povezanima s pristupom, primjerice zlouporabom ili povredama, i kako se oni istražuju.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 5.15 – zahtijeva formalizirane politike i postupke kontrole pristupa.

11.2. ISO/IEC 27002

11.2.1. Kontrole 5.15–5.17 – propisuju detaljne smjernice za pristup temeljen na ulogama, upravljanje životnim ciklusom korisnika i upravljanje povlaštenim pristupom.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-1 do AC-5 – zahtijevaju strukturirane politike za upravljanje pristupom, uključujući autorizaciju računa, pregled i praćenje.

11.4. GDPR EU

11.4.1. Članak 32 – zahtijeva tehničke i organizacijske kontrole, kao što je upravljanje pristupom, radi osiguravanja sigurnosti i povjerljivosti podataka.

11.5. Direktiva EU NIS2

11.5.1. Članak 21(2)(b) – propisuje operativne kontrole pristupa i sustave upravljanja identitetima radi sprječavanja neovlaštenog pristupa sustavima.

11.6. Uredba EU DORA

11.6.1. Članak 9 – naglašava sigurno upravljanje IKT rizicima, uključujući snažnu kontrolu pristupa za financijske subjekte.

11.7. COBIT 2019

11.7.1. APO07 – Upravljana sigurnost: zahtijeva definirane i provedene odgovornosti za pristup.

11.7.2. DSS01 – Upravljanje operacijama: uključuje postupke za upravljanje logičkim pristupom i održavanje sigurnih operativnih okruženja.