					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P04S					Naslov dokumenta: **Politika nadzora dostopa**							
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**

Usklajeno s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 5	
ISO/IEC 27002:2022	Kontrole: 5.15, 5.16, 5	
NIST SP 800-53 Rev. 5	AC-1 do AC-5	
GDPR EU	Člen 32	
NIS2 EU	Člen 21(2)(b)	
DORA EU	Člen 9	
COBIT 2019	APO07, DSS	

1. Namen

1.1. Ta politika določa način upravljanja dostopa do sistemov, podatkov in prostorov v organizaciji, da je dostop do informacij na podlagi poslovne potrebe omogočen izključno pooblaščenim osebam.

1.2. Določa jasna pravila za dodeljevanje, spreminjanje, spremljanje in ukinitev uporabniškega dostopa z namenom zmanjšanja tveganja nepooblaščenega dostopa ter zagotavljanja skladnosti z veljavnimi zakoni in standardi.

1.3. Ta politika uveljavlja načelo najmanjših privilegijev in zahteva, da je dostop omejen na najmanjši obseg, potreben za izvajanje delovnih nalog.

2. Področje uporabe

2.1. Ta politika velja za vse posameznike, ki uporabljajo ali upravljajo dostop do IT-sistemov, omrežij, podatkov ali prostorov organizacije, vključno z:

2.1.1. zaposlenimi

2.1.2. pogodbenimi izvajalci

2.1.3. začasnimi delavci

2.1.4. zunanjimi ponudniki IT-storitev

2.2. Politika zajema dostop do:

2.2.1. poslovnih aplikacij, skupne hrambe datotek in podatkovnih zbirk

2.2.2. elektronske pošte, VPN in sistemov za oddaljeni dostop

2.2.3. storitev v oblaku, ki se uporabljajo za poslovne namene

2.2.4. fizičnega dostopa do varovanih prostorov, kot so pisarne ali strežniške sobe

2.3. Ta politika se uporablja za vse naprave (naprave v lasti podjetja ali odobreni BYOD), platforme in lokacije.

3. Cilji

3.1. Zagotoviti, da se pravice dostopa dodelijo šele po formalni odobritvi na podlagi vloge in poslovne utemeljitve.

3.2. Preprečiti nepooblaščen ali prekomeren dostop do občutljivih podatkov, sistemov ali infrastrukture.

3.3. Določiti jasne postopke za dodeljevanje, spreminjanje in ukinitev uporabniškega dostopa.

3.4. Zahtevati redne preglede pravic dostopa ter samodejno ali ročno beleženje za podporo revizijskim postopkom.

3.5. Podpreti tehnično uveljavljanje omejitev dostopa z upravljanjem konfiguracij in spremljanjem.

4. Vloge in odgovornosti

4.1. Generalni direktor

4.1.1. odobri to politiko in zagotovi, da so na voljo sredstva za uvedbo učinkovitih kontrol dostopa.

4.1.2. odobri izjeme in pregleda letne revizije dostopa.

4.2. Vodja IT / zunanji ponudnik IT-storitev

4.2.1. izvaja dodeljevanje, spreminjanje in ukinitev uporabniških računov.

4.2.2. vodi evidenco nadzora dostopa za vse aktivnosti (ustvarjanje, spremembe, ukinitve).

4.2.3. uvaja kontrole dostopa na podlagi vlog (RBAC) in uveljavlja močno avtentikacijo (npr. MFA).

4.2.4. pregleduje dnevnike dostopa glede sumljivih dejavnosti in o ugotovitvah poroča 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. Letni pregled politike

9.1.1. Vodja IT mora to politiko pregledati letno. Vsaka sprememba pravnega, tehničnega ali organizacijskega okvira mora sprožiti takojšnjo posodobitev.

9.2. Sprožilci za pregled

9.2.1. Politiko je treba pregledati tudi, če nastopi kateri koli od naslednjih dogodkov:

9.2.2. večje spremembe sistemov ali migracije v oblak

9.2.3. spremembe vlog ali organizacijske strukture

9.2.4. varnostni incident, povezan z nepooblaščenim dostopom

9.2.5. regulatorne spremembe (npr. posodobitve GDPR, NIS2 ali DORA)

9.3. Dokumentiranje in sporočanje sprememb

9.3.1. Revizije morajo biti evidentirane z evidenco različic, odobritvijo generalnega direktorja in sporočene vsem zadevnim zaposlenim.

9.4. Dostopnost in usposabljanje

9.4.1. Ta politika mora biti dostopna vsem zaposlenim, ustrezno usposabljanje pa mora biti zagotovljeno ob uvajanju in nato letno.

10. Povezane politike in povezave

10.1. Ta politika se mora uporabljati usklajeno z naslednjimi politikami SME, da se zagotovi celovito uveljavljanje varnih praks dostopa:

10.1.1. P3S – Politika sprejemljive uporabe (AUP): zagotavlja, da uporabniki razumejo sprejemljivo ravnanje pri uporabi dodeljenega dostopa.

10.1.2. P5S – Politika upravljanja sprememb: zagotavlja, da so pravice dostopa usklajene z odobrenimi spremembami sistemov.

10.1.3. P7S – Politika uvajanja in prenehanja delovnega razmerja: določa sprožilne točke za dodeljevanje in ukinitev uporabniškega dostopa.

10.1.4. P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da so kontrole dostopa usklajene z varovali za osebne podatke.

10.1.5. P30S – Politika odzivanja na incidente: določa, kako se upravljajo in preiskujejo incidenti, povezani z dostopom (npr. zlorabe ali kršitve).

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 5.15 – zahteva formalizirane politike in postopke nadzora dostopa.

11.2. ISO/IEC 27002

11.2.1. Kontrole 5.15–5.17 – določajo podrobne smernice za dostop na podlagi vlog, upravljanje življenjskega cikla uporabnikov in upravljanje privilegiranega dostopa.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 do AC-5 – zahtevajo strukturirane politike upravljanja dostopa, vključno z odobravanjem računov, pregledovanjem in spremljanjem.

11.4. Uredba GDPR EU

11.4.1. Člen 32 – zahteva tehnične in organizacijske kontrole (kot je upravljanje dostopa) za zagotavljanje varnosti in zaupnosti podatkov.

11.5. Direktiva NIS2 EU

11.5.1. Člen 21(2)(b) – zahteva operativni nadzor dostopa in sisteme za upravljanje identitet za preprečevanje nepooblaščenega dostopa do sistemov.

11.6. Uredba DORA EU

11.6.1. Člen 9 – poudarja varno upravljanje IKT-tveganj, vključno z robustnim nadzorom dostopa za finančne subjekte.

11.7. COBIT 2019

11.7.1. APO07 – Upravljana varnost: zahteva opredeljene in uveljavljene odgovornosti glede dostopa.

11.7.2. DSS01 – Upravljanje operacij: vključuje postopke za upravljanje logičnega dostopa in vzdrževanje varnih operativnih okolij.