| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P04 | | | | | Naslov dokumenta:<br>**Politika nadzora dostopa** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>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** |
| | | | |
| | | | |

Usklajenost s standardi in predpisi

| Standard/predpis | Klavzula/člen | Komentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klavzule 5.15, 5.17, 5.18 | Upravljanje logičnega in fizičnega dostopa |
| ISO/IEC 27002:2022 | Kontrole 8.2, 8.3 | Dostop na podlagi vlog in upravljanje identitet |
| NIST SP 800-53 Rev. 5 | AC-1 do AC-20, IA-1 do IA-8 | Kontrole računov in dostopa, identiteta in avtentikacija |
| Uredba EU GDPR | Členi 5(1)(f), 32(1)(b); uvodna izjava 39 | Varstvo in minimizacija podatkov |
| Direktiva EU NIS2 | Člen 21(2)(c–e) | Nadzor dostopa, avtentikacija uporabnikov in zaščita sredstev |
| Uredba EU DORA | Členi 6, 9(2) | Dostop uporabnikov do IKT ter stroge kontrole za tretje osebe |
| COBIT 2019 | APO07, BAI03, DSS01, DSS05, MEA03 | Uvajanje, operacije, spremljanje in skladnost |

**1. Namen**

1.1 Ta politika določa obvezna načela, odgovornosti in zahteve glede kontrol za upravljanje dostopa do informacijskih sistemov, aplikacij, fizičnih objektov in informacijskih sredstev v celotni organizaciji.

1.2 Zagotavlja, da se dostop dodeljuje na podlagi poslovne potrebe, delovne funkcije in profila tveganja ter uveljavlja načelo najmanjših privilegijev, potrebo po seznanitvi in ločevanje dolžnosti (SoD).

1.3 Politika podpira izvajanje okvira sistema upravljanja informacijske varnosti ter izpolnjevanje zahtev standarda ISO/IEC 27001:2022, klavzule 5.15, in povezanih kontrol, ki urejajo logični in fizični dostop, avtentikacijo uporabnikov ter upravljanje življenjskega cikla dostopa.

1.4 Ta politika predstavlja temelj za zaščito digitalnih in fizičnih virov pred nepooblaščeno uporabo, zlorabo ali ogrožanjem.

**2. Obseg**

**2.1 Ta politika velja za vse uporabnike, sisteme in objekte znotraj obsega ISMS, vključno z:**

2.1.1 zaposlenimi, pogodbenimi izvajalci, dobavitelji in začasnimi delavci,

2.1.2 lokalno infrastrukturo, sistemi v oblaku in hibridnimi okolji,

2.1.3 vsemi sredstvi podjetja — strojno opremo, programsko opremo, podatki in varovanimi fizičnimi območji,

2.1.4 logičnim dostopom (npr. sistemi, omrežja, aplikacije, vmesniki API) in fizičnim dostopom (npr. zgradbe, podatkovni centri).

2.2 Ureja dostop skozi celoten življenjski cikel identitete in uporabe virov, od uvajanja in dodelitve dostopa do sprememb vlog in prenehanja.

2.3 Politika zajema tudi uporabo lastnih naprav in oddaljeni dostop ter zagotavlja, da se kontrole dosledno izvajajo ne glede na lokacijo in model lastništva naprav.

**3. Cilji**

3.1 Uvesti varne kontrole dostopa na podlagi vlog, ki podpirajo operativno celovitost in regulativno skladnost.

3.2 Zagotoviti, da so pravice dostopa ustrezno odobrene, spremljane in pravočasno preklicane.

3.3 Preprečiti nepooblaščen dostop, povišanje pravic ali ohranjanje zastarelih pravic dostopa.

3.4 Podpreti načela ničelnega zaupanja tako, da je dostop privzeto zavrnjen, razen če je izrecno odobren in utemeljen.

3.5 Zagotoviti presojevalcem in zainteresiranim stranem ustrezna zagotovila z uporabo dokazno podprtih, avtomatiziranih pregledov dostopa in izvajanja politike.

3.6 Vgraditi nadzor dostopa v poslovne procese, dogodke v kadrovskem življenjskem ciklu in tehnične arhitekture.

## 4. Vloge in odgovornosti

### 4.1 Najvišje vodstvo

4.1.1 Potrdi politiko nadzora dostopa ter zagotovi ustrezen proračun in kadrovske vire za njeno izvajanje.

4.1.2 V okviru vodstvenih pregledov obravnava tveganja, povezana z nadzorom dostopa, in na strateški ravni določa odgovornost.

### 4.2 Vodja informacijske varnosti / vodja ISMS

4.2.1 Je lastnik okvira nadzora dostopa in zagotavlja usklajenost z ISO/IEC 27001 ter povezanimi standardi.

4.2.2 Usklajuje izvajanje politike, testiranje kontrol, odpravo pomanjkljivosti in poročanje o kazalnikih nadzora dostopa.

4.2.3 Nadzira modeliranje dostopa na podlagi tveganja in spremlja vrzeli v sistemu kontrol.

[ ... 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 Sprožilci pregleda in pogostost

#### 9.1.1 Ta politika mora biti pregledana:

9.1.1.1 letno ali

9.1.1.2 po večji spremembi IT-infrastrukture, regulativnih zahtev ali profila tveganja,

9.1.1.3 po incidentih, ki razkrijejo slabosti v kontrolah dostopa,

9.1.1.4 kadar pride do pomembnih sprememb v tehnologijah avtentikacije ali platformah za upravljanje identitet.

### 9.2 Pristojnost in postopek pregleda

#### 9.2.1 Vodja informacijske varnosti ali imenovani vodja ISMS upravlja cikel pregleda, pri čemer upošteva:

9.2.1.1 ugotovitve notranje revizije,

9.2.1.2 rezultate in kazalnike pregledov dostopa,

9.2.1.3 pravne in regulativne posodobitve,

9.2.1.4 spremembe tehnoloških platform.

9.2.2 Vse spremembe mora odobriti najvišje vodstvo in jih sporočiti vsem zainteresiranim stranem.

9.2.3 Prizadeti uporabniki bodo ob bistvenih posodobitvah morda morali ponovno potrditi seznanjenost s politiko.

### 9.3 Obvladovanje različic in dokumentacija

#### 9.3.1 Izvirna različica mora biti shranjena v repozitoriju dokumentacije ISMS z naslednjimi metapodatki:

9.3.1.1 številka različice in evidenca sprememb,

9.3.1.2 datum začetka veljavnosti in datum naslednjega pregleda,

9.3.1.3 lastnik in organ odobritve,

9.3.1.4 distribucija in evidenca potrditev.

9.3.2 Nadomeščene različice morajo biti arhivirane in dostopne najmanj 3 leta.

**10. Povezane politike in povezave**

**10.1 To politiko je treba razlagati skupaj z naslednjimi politikami, od katerih je funkcionalno odvisna:**

10.1.1 P01 – Politika informacijske varnosti: določa zavezanost organizacije varnosti ter pričakovanja na visoki ravni glede nadzora dostopa.

10.1.2 P03 – Politika sprejemljive uporabe (AUP): določa vedenjska pravila za dostop in odgovornost uporabnikov za odgovorno uporabo sistemov.

10.1.3 P05 – Politika upravljanja sprememb: ureja, kako je treba spremembe konfiguracij dostopa, vlog ali skupinskih struktur varno uvesti in preizkusiti.

10.1.4 P07 – Politika uvajanja in prenehanja: določa dodelitev in preklic pravic dostopa v skladu z dogodki življenjskega cikla uporabnika.

10.1.5 P11 – Politika upravljanja uporabniških računov in privilegijev: operacionalizira kontrole na ravni računov in dopolnjuje to politiko s smernicami za tehnično izvajanje nadzora dostopa.

10.2 Te politike skupaj zagotavljajo skladen in izvršljiv okvir upravljanja pravic dostopa v vseh poslovnih enotah in tehnologijah.

**11. Referenčni standardi in okviri**

**11.1 ISO/IEC 27001:2022:**

11.1.1 Klavzula 5.15 – Nadzor dostopa: ta politika izpolnjuje zahtevo po nadzoru dostopa do informacij in drugih povezanih sredstev na podlagi poslovnih zahtev in zahtev informacijske varnosti.

11.1.2 Klavzula 5.17 – Upravljanje identitet in klavzula 5.18 – Informacije za avtentikacijo: ti zahtevi se izvajata prek dodeljevanja identitet, mehanizmov avtentikacije in dodeljevanja privilegijev.

11.1.3 Kontrole Priloge A 8.2 (Nadzor dostopa) in 8.3 (Upravljanje identitet): zagotavljajo temelj za cilje kontrol te politike, vključno z dostopom na podlagi vlog, integracijo življenjskega cikla uporabnikov in zaščito privilegiranega dostopa.

**11.2 NIST SP 800-53 Rev. 5:**

11.2.1 Družina AC (AC-1 do AC-20): ta politika podpira zahteve NIST glede nadzora dostopa za fizične in logične sisteme, vključno z opredelitvijo politike (AC-1), upravljanjem računov (AC-2) in ločevanjem dolžnosti (AC-5).

11.2.2 Družina IA (IA-1 do IA-8): zagotavlja smernice za avtentikacijo identitete, zaščito poverilnic in MFA.

11.2.3 AU-2, AU-12: zahteve glede beleženja in revidiranja, ki jih uveljavlja ta politika, podpirajo odgovornost uporabnikov in preiskovanje incidentov.

11.2.4 PE-2 do PE-6: obravnavajo omejitve fizičnega dostopa, ki jih ta politika delno uveljavlja prek kontrol vstopnih kartic in dovoljenj za dostop do objektov.

**11.3 Uredba EU GDPR (2016/679):**

11.3.1 Člen 5(1)(f): osebni podatki morajo biti zaščiteni pred nepooblaščenim dostopom. Ta politika zagotavlja tehnično in postopkovno izvajanje tega načela.

11.3.2 Člen 32(1)(b): zahteva uvedbo kontrol dostopa, psevdonimizacije in šifriranja za preprečevanje nepooblaščene obdelave osebnih podatkov.

11.3.3 Uvodna izjava 39: zahteva minimizacijo dostopa do osebnih podatkov, kar se v tej politiki uveljavlja z načelom najmanjših privilegijev in zahtevami po utemeljitvi dostopa.

**11.4 Direktiva EU NIS2 (2022/2555):**

11.4.1 Člen 21(2)(c–e): ta politika omogoča tehnične in organizacijske ukrepe za nadzor dostopa, avtentikacijo uporabnikov in zaščito sredstev pri bistvenih in pomembnih subjektih.

**11.5 Uredba EU DORA (2022/2554):**

11.5.1 Člen 6: zahteva politike upravljanja tveganj IKT, ki izrecno vključujejo upravljanje uporabniškega dostopa in kontrole življenjskega cikla identitet. Ta politika izpolnjuje to zahtevo za finančni sektor in sektor storitev IKT.

11.5.2 Člen 9(2): ta politika podpira uveljavljanje strogih kontrol dostopa kot dela upravljanja storitev IKT tretjih oseb in storitev znotraj skupine.

**11.6 COBIT 2019:**

11.6.1 APO07 – Upravljani človeški viri: uveljavlja kontrole uvajanja in izstopa v podporo upravljanju pravic dostopa.

11.6.2 BAI03 – Upravljana identifikacija in izgradnja rešitev: vključuje zahteve nadzora dostopa v zasnovo sistemov in procese sprememb.

11.6.3 DSS01 – Upravljane operacije in DSS05 – Upravljane varnostne storitve: urejata uveljavljanje omejitev logičnega dostopa in spremljanje kršitev.

11.6.4 MEA03 – Spremljanje, vrednotenje in ocenjevanje skladnosti: podpira revizijske mehanizme in mehanizme zagotavljanja za preverjanje učinkovitosti nadzora dostopa.