| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P03 | | | | | Naslov dokumenta:<br>**Politika sprejemljive uporabe** | | | | | | | |
| 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 | Klavzula 5 | Določa vedenjske norme in zahteve za Politiko sprejemljive uporabe (AUP) |
| ISO/IEC 27002:2022 | Kontrole 6.1, 6.2, 8.1, 8.12 | Usmerja odgovornosti za informacijsko varnost, ozaveščanje ter upravljanje naprav in podatkov |
| NIST SP 800-53 Rev.5 | AC-19, AC-20, AT-2 | Nadzor dostopa ter kontrole ozaveščanja in vedenja, pomembne za uporabo IT-sredstev podjetja |
| EU GDPR | Členi 5(1)(f), 32; uvodna izjava 39 | Zahteva zaupnost in celovitost, določa tehnične in organizacijske ukrepe ter pravne podlage za ustrezno uporabo |
| EU NIS2 | Člen 21(2)(a–d) | Določa operativne politike in usposabljanje za varno uporabo |
| EU DORA | Člen 5 | Podpira upravljanje IKT-tveganj z urejanjem vedenja uporabnikov |
| COBIT 2019 | APO07, BAI05, DSS05, MEA01 | Človeški viri, upravljanje sprememb, upravljane varnostne storitve ter spremljanje skladnosti in uspešnosti |

**1. Namen**

1.1 Ta politika določa sprejemljivo in nesprejemljivo uporabo informacijskih sistemov organizacije, računalniških virov, komunikacijskih orodij in praks ravnanja s podatki.

1.2 Zagotavlja, da vsi uporabniki razumejo svoje odgovornosti pri uporabi IT-sredstev podjetja ter da njihova ravnanja podpirajo zaupnost, celovitost in razpoložljivost (CIA) ter zakonito obdelavo informacij.

1.3 Politika izpolnjuje zahteve ISO/IEC 27001:2022, točka 5.10, tako da določa vedenjske norme za uporabo sistemov ter uvaja tehnične in postopkovne varovalne ukrepe za zmanjšanje tveganja zlorabe, malomarnosti ali neprimerne uporabe.

1.4 Podpira tudi preiskovalne dejavnosti in izvršilne ukrepe, vključno z odzivanjem na incidente in disciplinskimi ukrepi ob kršitvah.

**2. Obseg**

**2.1 Ta politika velja za vse posameznike in subjekte, ki jim je odobren dostop do informacijskih sistemov in sredstev organizacije, vključno z, vendar ne omejeno na:**

2.1.1 zaposlene, pogodbene izvajalce, svetovalce, praktikante in agencijsko osebje,

2.1.2 dobavitelje tretjih oseb z dostopom do sistemov ali dodeljenimi administrativnimi vlogami,

2.1.3 goste ali partnerje, ki uporabljajo IT-infrastrukturo v lasti organizacije ali odobreno IT-infrastrukturo.

**2.2 Obseg vključuje vsa tehnološka in podatkovna sredstva organizacije, vključno z:**

2.2.1 delovnimi postajami, prenosniki, mobilnimi napravami in strežniki,

2.2.2 omrežno infrastrukturo in storitvami v oblaku,

2.2.3 e-pošto, sporočanjem, hrambo datotek, platformami za sodelovanje in VPN,

2.2.4 podatki v mirovanju, med prenosom ali obdelavo, ne glede na obliko ali lokacijo,

2.2.5 vsemi osebnimi napravami, ki se uporabljajo v okviru dogovora o uporabi lastnih naprav (BYOD) in se povezujejo z organizacijskimi sistemi.

**2.3 Ta politika se uporablja v vseh delovnih okoljih, vključno z:**

2.3.1 poslovnimi prostori podjetja in proizvodnimi lokacijami,

2.3.2 lokacijami za delo na daljavo ali hibridnimi oblikami dela,

2.3.3 terenskim delom ali prostori, ki jih upravljajo tretje osebe.

2.4 Vsi uporabniki morajo to politiko potrditi in jo upoštevati kot pogoj za dostop do sistemov podjetja ali ravnanje s podatki podjetja.

**3. Cilji**

3.1 Določiti in uveljaviti pravila za pooblaščeno uporabo IT-virov.

3.2 Preprečiti nepooblaščen dostop, uhajanje podatkov ali škodo zaradi malomarne ali zlonamerne uporabe.

3.3 Zaščititi omrežja, sredstva in podatke podjetja pred grožnjami, ki izhajajo iz vedenja uporabnikov.

3.4 Podpreti pravne in pogodbene obveznosti z izkazovanjem skrbnega ravnanja pri upravljanju IT-virov.

3.5 Zagotoviti doslednost in jasnost pri uporabi disciplinskih ukrepov in postopkov upravljanja izjem.

3.6 Spodbujati kulturo etične, varne in odgovorne uporabe digitalnih in fizičnih računalniških virov.

**4. Vloge in odgovornosti**

**4.1 Najvišje vodstvo**

4.1.1 Odobri Politiko sprejemljive uporabe (AUP) in zagotovi njeno usklajenost s poslovnimi cilji, regulativnimi zahtevami in vrednotami organizacije.

4.1.2 Dodeli vire za izvajanje, usposabljanje, spremljanje in pregled politike.

4.1.3 V okviru upravljanja ISMS pregleduje stanje skladnosti in disciplinske ukrepe, povezane s kršitvami politike.

**4.2 IT in ekipe informacijske varnosti**

4.2.1 Uvedejo tehnične varovalne ukrepe za izvajanje te politike, vključno z:

4.2.2 filtriranjem vsebin, zaščito pred zlonamerno programsko opremo, varnostjo končnih točk in orodji za spremljanje omrežja,

4.2.3 varnostnimi konfiguracijami e-pošte in rešitvami za preprečevanje izgube podatkov (DLP),

4.2.4 seznami blokiranih in dovoljenih programov, strojne opreme in spletnih mest,

4.2.5 vzdrževanjem popisa odobrene in prepovedane programske opreme, naprav in storitev.

4.2.6 Preiskujejo sume kršitev AUP, zbirajo forenzične dokaze in po potrebi podpirajo disciplinske ali pravne ukrepe.

4.2.7 Sodelujejo s kadrovsko in pravno službo pri obravnavi incidentov, eskalaciji in obveznostih poročanja.

[ ... 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 Povodi za pregled in pogostost**

**9.1.1 Ta politika se pregleda:**

9.1.1.1 najmanj enkrat letno,

9.1.1.2 po vsaki pomembni spremembi tehnologije ali infrastrukture,

9.1.1.3 po incidentih ali ugotovitvah presoje, ki izpostavijo vrzeli pri izvajanju,

9.1.1.4 kot odziv na spremembe veljavne zakonodaje ali pogodbenih obveznosti.

**9.2 Lastništvo in odobritev**

9.2.1 Za postopek pregleda je odgovoren vodja informacijske varnosti (CISO) ali imenovani vodja ISMS.

9.2.2 Posodobitve mora odobriti najvišje vodstvo, o njih pa je treba obvestiti celotno organizacijo.

9.2.3 Potrditev posodobljenih določil mora biti ponovno pridobljena ob ponovni izdaji politike.

**9.3 Upravljanje dokumenta**

**9.3.1 Politika mora vključevati naslednje metapodatke in podatke o verzioniranju:**

9.3.1.1 naslov, identifikator in stopnjo klasifikacije,

9.3.1.2 lastnika politike in skrbnika dokumenta,

9.3.1.3 zgodovino sprememb in utemeljitev posodobitev,

9.3.1.4 datume pregledov in naslednje načrtovane posodobitve,

9.3.1.5 sklice na distribucijske dnevnike in dnevnike potrditev.

9.3.2 Izvirnik mora biti hranjen v repozitoriju dokumentacije ISMS pod nadzorom različic.

**10. Povezane politike in povezave**

**10.1 To politiko je treba razlagati skupaj z naslednjimi politikami:**

10.1.1 P1 – Politika informacijske varnosti: določa temeljna pričakovanja glede vedenja in zavezanost najvišjega vodstva sprejemljivi uporabi.

10.1.2 P4 – Politika nadzora dostopa: določa dovoljenja in pravice, povezane z dostopom uporabnikov, sistemov in podatkov, ter neposredno uveljavlja meje sprejemljive uporabe.

10.1.3 P6 – Politika obvladovanja tveganj: obravnava tveganja, povezana z vedenjem, ter podpira dejavnosti spremljanja in obravnave groženj, ki izhajajo iz ravnanja uporabnikov.

10.1.4 P7 – Politika uvajanja in prenehanja sodelovanja: zagotavlja, da so pogoji sprejemljive uporabe potrjeni ob nastopu in preklicani ob odhodu.

10.1.5 P9 – Politika dela na daljavo: razširja določila sprejemljive uporabe na oddaljeno in hibridno delovno okolje.

10.2 Te povezane politike tvorijo večplastni obrambni model za vedenjsko, tehnično in pogodbeno upravljanje.

**11. Referenčni standardi in okviri**

11.1 Ta Politika sprejemljive uporabe (AUP) je usklajena z mednarodno priznanimi standardi in pravnimi okviri, da zagotavlja izvršljive, preverljive in na tveganjih temelječe vedenjske kontrole pri vseh oblikah uporabe digitalnih in fizičnih informacijskih sistemov.

**11.2 ISO/IEC 27001:2022**

11.2.1 Točka 5.10 – Sprejemljiva uporaba informacij in drugih povezanih sredstev: ta politika neposredno izpolnjuje zahtevo po določitvi, sporočanju in uveljavljanju pravil, ki urejajo ustrezno uporabo IT-virov.

11.2.2 Priloga A, kontrola 6.1 – Odgovornost za informacijsko varnost: dodeljuje jasne odgovornosti glede vedenja uporabnikov in nadzora nad skladnostjo.

11.2.3 Priloga A, kontrola 6.2 – Ozaveščanje, izobraževanje in usposabljanje za informacijsko varnost: vgrajeni procesi usposabljanja in potrjevanja politike so del izvajanja AUP.

11.2.4 Priloga A, kontroli 8.1 – Naprave končnih uporabnikov in 8.12 – Preprečevanje izgube podatkov (DLP): obravnavata sprejemljivo vedenje na napravah uporabnikov in urejata dejavnosti, ki bi lahko povzročile razkritje ali uhajanje podatkov.

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

11.3.1 AC-19 (nadzor dostopa za mobilne naprave) in AC-20 (uporaba zunanjih informacijskih sistemov): ta politika določa obveznosti in omejitve uporabnikov za BYOD ter dostop do sistemov tretjih oseb.

11.3.2 PL-4 (pravila vedenja): določa podrobne zahteve sprejemljive uporabe, skladne s to politiko.

11.3.3 AT-2 (usposabljanje za varnostno ozaveščanje): podprto z usposabljanjem uporabnikov in dokumentirano potrditvijo politike.

11.3.4 AU-2 (revizijski dogodki) in AU-12 (ustvarjanje revizijskih zapisov): izvajanje temelji na spremljanju dejanj uporabnikov in opozarjanju na kršitve.

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

11.4.1 Člen 5(1)(f): zagotavlja varnost in celovitost osebnih podatkov; ta politika zmanjšuje tveganja, ki izhajajo iz človeškega vedenja in nepooblaščene uporabe.

11.4.2 Člen 32: določa tehnične in organizacijske ukrepe, kot so vedenjske kontrole in omejitve uporabe, za zaščito osebnih podatkov.

11.4.3 Uvodna izjava 39: poudarja potrebo po zagotavljanju le nujnega dostopa in zakonite uporabe podatkov s strani pooblaščenih posameznikov.

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

11.5.1 Člen 21(2)(a–d): zahteva operativne politike in usposabljanje za varno uporabo sistemov, kar ta AUP zagotavlja z določitvijo vedenja, spremljanja in postopkov uveljavljanja.

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

11.6.1 Člen 5: ta politika podpira okvir upravljanja IKT-tveganj z določitvijo pravil za interakcijo med človekom in sistemom ter zmanjševanjem izpostavljenosti kibernetskim tveganjem, povezanim z vedenjem.

**11.7 COBIT 2019:**

11.7.1 APO07 – Upravljani človeški viri: uveljavlja odgovornosti uporabnikov in ozaveščanje skozi celoten življenjski cikel zaposlenega.

11.7.2 BAI05 – Upravljana organizacijska sprememba: vključuje upravljanje sprejemljive uporabe v procese sprememb, ki vplivajo na vedenje uporabnikov.

11.7.3 DSS05 – Upravljane varnostne storitve: podpira spremljanje dejavnosti uporabnikov, vedenjska opozorila in samodejne mehanizme odziva.

11.7.4 MEA01 – Spremljanje, vrednotenje in ocenjevanje uspešnosti ter skladnosti: politika določa kazalnike in mehanizme za preverjanje skladnosti uporabnikov z vedenjskimi pričakovanji.