					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P03S					Naslov dokumenta: **Politika sprejemljive uporabe (AUP)**							
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	Relevantno za celoten obseg politike in njeno izvajanje
ISO/IEC 27002:2022	5.10, 5.11, 5	Smernice glede zahtev in kontrol za sprejemljivo uporabo
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Obravnava uporabo sistemov in naprav, spremljanje ter usposabljanje uporabnikov
Uredba EU GDPR	Člena 5(1)(f), 32	Celovitost in zaupnost podatkov ter varnostni ukrepi
Direktiva EU NIS2	Člen 21(2)(b)	Zahteva ustrezne varnostne politike in politiko sprejemljive uporabe (AUP)
Uredba EU DORA	Člen 9	Politika upravljanja tveganj IKT, kontrole in izvajanje
COBIT 2019	DSS05, BAI08	Varnostne storitve in upravljanje znanja

1. Namen

1.1. Ta politika določa sprejemljivo, odgovorno in varno uporabo sistemov, naprav, dostopa do interneta, e-pošte, storitev v oblaku ter vseh naprav v osebni lasti, ki se uporabljajo za poslovne namene in jih zagotovi podjetje oziroma odobri za poslovno uporabo.

1.2. Zagotavlja, da posamezniki razumejo svoje obveznosti pri uporabi organizacijskih virov IT ter pri varovanju celovitosti podatkov, zasebnosti in neprekinjenega poslovanja.

1.3. Ta politika podpira skladnost z ISO/IEC 27001:2022 z uveljavljanjem jasnih standardov vedenja uporabnikov, usklajenih s pravnimi, pogodbenimi in regulativnimi zahtevami.

2. Področje uporabe

2.1. Ta politika velja za vse posameznike, ki dostopajo do sistemov ali podatkov podjetja, jih upravljajo ali z njimi delajo, vključno z:

2.1.1. zaposlenimi in pogodbenimi izvajalci,

2.1.2. začasnimi delavci ali praktikanti,

2.1.3. zunanjimi ponudniki IT-storitev.

2.2. Politika zajema:

2.2.1. računalnike, telefone in tablice v lasti podjetja,

2.2.2. naprave v osebni lasti, odobrene za poslovno uporabo (BYOD),

2.2.3. omrežja podjetja, platforme v oblaku in programske storitve,

2.2.4. dostop do interneta, e-poštne sisteme, skupno shranjevanje in poslovne aplikacije.

2.3. Ta politika velja v vseh delovnih okoljih — na lokaciji podjetja, pri delu na daljavo in v hibridnem načinu — ter v vseh delovnih urah.

3. Cilji

3.1. Določiti, kaj pomeni sprejemljiva in nesprejemljiva uporaba IT-sistemov.

3.1.1. Zmanjšati varnostna tveganja, ki izhajajo iz zlorabe, nepooblaščenega dostopa ali vnosa zlonamerne programske opreme.

3.1.2. Zaščititi poslovne podatke, podatke o strankah in ugled podjetja.

3.1.3. Določiti izvršljiva pravila in zagotoviti odgovornost vseh uporabnikov.

3.1.4. Podpreti spremljanje in skladnost za zgodnje odkrivanje kršitev ter izvajanje korektivnih ukrepov.

4. Vloge in odgovornosti

4.1. Generalni direktor

4.1.1. Odobri to politiko in je odgovoren za zagotovitev virov in pooblastil za njeno izvajanje.

4.1.2. Pregleda in odobri vse izjeme od te politike.

4.2. Vodja IT ali zunanji ponudnik IT-storitev

4.2.1. Vzdržuje sezname odobrene programske opreme in odobrene strojne opreme.

4.2.2. Konfigurira naprave za uveljavljanje pravil sprejemljive uporabe (npr. filtriranje vsebin, revizijsko beleženje dostopa).

4.2.3. Spremlja uporabo zaradi morebitnih kršitev in preiskuje incidente.

4.2.4. Zagotavlja, da so naprave v osebni lasti (BYOD), če se uporabljajo za poslovne namene, odobrene in varno konfigurirane.

[... 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

9.1.1. To politiko mora letno pregledati vodja IT, končno odobritev pa poda generalni direktor, da se zagotovi njena usklajenost z vzorci uporabe tehnologije, nastajajočimi tveganji in obveznostmi glede skladnosti.

9.2. Sprožilci vmesnega pregleda

9.2.1. Pregledi se morajo izvesti tudi kot odziv na:

9.2.2. nove sisteme ali tehnologije (npr. nova storitev v oblaku ali platforma končnih točk),

9.2.3. pomembne kršitve politike,

9.2.4. posodobljeno zakonodajo ali pogodbene pogoje, ki vplivajo na uporabo IT.

9.3. Dokumentiranje sprememb

9.3.1. Vse posodobitve morajo biti zabeležene v evidenci različic, ki vključuje:

9.3.1.1. številko različice,

9.3.1.2. datum pregleda,

9.3.1.3. povzetek sprememb,

9.3.1.4. organ odobritve.

9.4. Komuniciranje politike

9.4.1. Posodobljene različice te politike morajo biti posredovane vsem zadevnim uporabnikom. Zaposleni morajo potrditi prejem in razumevanje v okviru svojih obveznosti glede varnostnega ozaveščanja.

10. Povezane politike in povezave

10.1. Ta politika se uporablja skupaj z več drugimi politikami za mala in srednja podjetja, da se zagotovi celovita pokritost varnostnih odgovornosti:

10.1.1. P4S – Politika nadzora dostopa: določa tehnično in postopkovno uveljavljanje dovoljene uporabe ter omejitev računov.

10.1.2. P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja usposabljanje uporabnikov o mejah sprejemljive uporabe in obveznostih poročanja.

10.1.3. P9S – Politika dela na daljavo: ureja uporabo sistemov podjetja pri delu zunaj lokacije ali od doma.

10.1.4. P17S – Politika varstva podatkov in zasebnosti: uveljavlja pravila ravnanja z osebnimi podatki, ki se prekrivajo s spremljanjem sprejemljive uporabe in BYOD.

10.1.5. P30S – Politika odzivanja na incidente: ureja postopke za preiskavo in odzivanje na zlorabe ali kršitve pravil sprejemljive uporabe.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 5.10 – Od organizacij zahteva, da opredelijo in uveljavijo sprejemljivo uporabo informacijskih sredstev.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.10 – Podaja smernice za sprejemljivo uporabo sistemov, vključno z dovoljenimi in prepovedanimi ravnanji.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Obravnava nadzor uporabe sistemov, vključno z napravami v osebni lasti.

11.3.2. AC-20 – Zahteva odobritev in spremljanje zunanjih sistemov.

11.3.3. AT-2 – Poudarja usposabljanje uporabnikov o praksah sprejemljive uporabe.

11.4. Uredba EU GDPR

11.4.1. Člen 5(1)(f) – Zahteva celovitost in zaupnost osebnih podatkov, ki ju lahko ogrozi zloraba s strani uporabnikov.

11.4.2. Člen 32 – Zahteva uvedbo tehničnih in organizacijskih ukrepov za zaščito sistemov in podatkov.

11.5. Direktiva EU NIS2

11.5.1. Člen 21(2)(b) – Zahteva ustrezne varnostne politike, vključno s pravili sprejemljive uporabe, za zmanjševanje kibernetskih groženj.

11.6. Uredba EU DORA

11.6.1. Člen 9 – Zahteva politike upravljanja tveganj IKT, ki vključujejo kontrole uporabe in mehanizme izvajanja.

11.7. COBIT 2019

11.7.1. DSS05 – Upravljanje varnostnih storitev: poudarja nadzor vedenja uporabnikov na podlagi politik.

11.7.2. BAI08 – Upravljanje znanja: obravnava ozaveščenost o odgovornostih iz politike in usposabljanje o sprejemljivi uporabi.