					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P34S					Naslov dokumenta: **Politika mobilnih naprav in uporabe lastnih naprav**							
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**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzule 5.1, 5.2, 6.1, 6.2, 8	Splošne zahteve ISMS ter zahteve glede kontrol za mobilne naprave in uporabo lastnih naprav
ISO/IEC 27002:2022	Kontrole 5.10–5.13	Podrobne kontrole za mobilne naprave, uporabo lastnih naprav in oddaljeni dostop
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Kontrole za naprave, medije in konfiguracijo v zveznem okolju
EU GDPR	Člen 5(1)(f)	Varstvo osebnih podatkov in zaščita mobilnih končnih točk
EU NIS2	Člen 21(2)(d)	Zaščita poslovno kritičnih naprav, vključno z uporabo lastnih naprav
EU DORA	Členi 9, 10	Tveganja IKT in neprekinjenost poslovanja za mobilne končne točke
COBIT 2019	APO13, DSS01, DSS05	Upravljanje IT, operacij in kontrol varnostnih storitev

1. Namen

1.1. Ta politika določa obvezne varnostne zahteve za uporabo mobilnih naprav, vključno s pametnimi telefoni, tablicami in prenosnimi računalniki, pri dostopu do informacij, sistemov ali storitev podjetja.

1.2. Ureja tudi uporabo lastnih naprav, da se zagotovi varstvo podatkov strank in poslovnih podatkov ne glede na lastništvo naprave.

1.3. Politika zagotavlja dosledne zaščitne ukrepe za mobilni dostop, podpira doseganje ciljev certifikacije po ISO/IEC 27001 ter preprečuje izgubo podatkov ali kompromitacijo zaradi izgubljenih, ukradenih ali neustrezno uporabljenih mobilnih končnih točk.

1.4. Zagotavlja, da se pri uporabi mobilnih naprav v MSP brez namenskih IT-ekip uporabljajo tehnični in postopkovni zaščitni ukrepi, vključno z okolji za delo na daljavo in storitvami v oblaku.

2. Področje uporabe

2.1. Ta politika velja za vse zaposlene, pogodbene izvajalce, praktikante in ponudnike storitev, ki:

2.1.1. uporabljajo mobilno napravo za dostop do podatkov ali sistemov podjetja oziroma za njihovo obdelavo ali hrambo,

2.1.2. se povezujejo s storitvami podjetja, vključno z e-pošto, deljenimi mapami, aplikacijami v oblaku ali notranjimi sistemi prek VPN.

2.2. Politika zajema:

2.2.1. vse mobilne naprave: pametne telefone, tablice in prenosne računalnike (naprave v lasti podjetja ali osebne naprave v okviru uporabe lastnih naprav),

2.2.2. vse operacijske sisteme (npr. iOS, Android, Windows, macOS),

2.2.3. vse lokacije (pisarna, dom, delo na daljavo, javni prostori).

2.3. Politika velja v vseh delovnih okoljih in se mora izvajati ne glede na lastništvo naprave.

3. Cilji

3.1. Preprečevanje izgube podatkov: zagotoviti, da uporaba mobilnih naprav ne izpostavi občutljivih podatkov podjetja ali strank nepooblaščenemu dostopu, kraji ali neustrezni uporabi.

3.2. Jasna pravila za uporabo lastnih naprav: določiti izvršljive pogoje za uporabo osebnih naprav v poslovne namene ter zagotoviti pravne in tehnične zaščitne ukrepe.

3.3. Podpora regulativni skladnosti: izpolnjevati zahteve po ISO/IEC 27001, GDPR, NIS2 in drugih pravnih obveznostih z izvršljivimi praksami varnosti mobilnih naprav.

3.4. Zmanjševanje operativnega tveganja: zmanjšati verjetnost operativnih motenj zaradi neustrezne uporabe, kompromitacije ali odpovedi mobilnih naprav.

3.5. Ohranjanje zaupanja strank: strankam in partnerjem izkazati, da njihovi podatki ostajajo zaščiteni tudi pri dostopu prek mobilnih ali osebnih naprav.

4. Vloge in odgovornosti

4.1. Generalni direktor (GM):

4.1.1. je odgovoren za to politiko,

4.1.2. odobri vsako uporabo mobilnega dostopa in uporabo lastnih naprav za dostop do sistemov podjetja,

4.1.3. zagotovi, da so dogovori o uporabi lastnih naprav podpisani, shranjeni in spremljani,

4.1.4. preveri, da zunanji ponudniki IT-storitev izvajajo zahtevane zaščitne ukrepe za mobilne naprave.

4.2. Imenovano osebje ali IT-podpora:

4.2.1. pomaga pri nastavitvi, registraciji in konfiguraciji mobilnih naprav, ki se uporabljajo za delo,

4.2.2. uveljavlja kontrole dostopa, omejitve aplikacij in politike spremljanja, povezane z mobilnimi napravami,

4.2.3. podpira odzivanje na incidente, povezane z mobilnimi napravami (izgubljene, ukradene ali kompromitirane naprave).

[... 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. Generalni direktor (GM) mora to politiko pregledati najmanj enkrat na 12 mesecev.

9.1.2. Pregled mora potrditi nadaljnjo usklajenost z zahtevami ISO/IEC 27001, razvojem mobilnih tehnologij in spremembami poslovanja.

9.1.3. Pri posodobitvah je treba upoštevati tudi nedavne incidente, rezultate presoj ali regulativni razvoj (npr. GDPR, NIS2, DORA).

9.2. Sprožilni dogodki za vmesni pregled

9.2.1. Ta politika se mora nemudoma posodobiti, če nastopi kateri koli od naslednjih dogodkov:

9.2.1.1. večji varnostni incident, povezan z mobilnimi napravami (npr. kršitev zaradi izgubljene ali vdrte naprave),

9.2.1.2. sprememba podprtih platform ali orodij za upravljanje mobilnih naprav,

9.2.1.3. pravna ali regulativna sprememba, ki vpliva na uporabo osebnih naprav ali varstvo podatkov,

9.2.1.4. uvedba novih aplikacij, storitev ali orodij tretjih oseb, ki se uporabljajo na mobilnih napravah.

9.3. Dokumentiranje sprememb

9.3.1. Vsi pregledi in posodobitve morajo biti dokumentirani, vključno z datumom pregleda, izvedenimi spremembami in odobritvijo GM.

9.3.2. Za namene revizije se mora hraniti evidenca nadzora različic.

9.4. Obveščanje in dostop

9.4.1. GM mora zagotoviti, da so vsi uporabniki (zaposleni, pogodbene izvajalce, tretje osebe) obveščeni o spremembah.

9.4.2. Posodobljene različice morajo biti enostavno dostopne, na primer v deljenih mapah ali na notranjih platformah.

10. Povezane politike in povezave

10.1. Ta politika je del celotnega nabora politik informacijske varnosti za MSP in se mora izvajati skupaj z naslednjimi politikami:

10.1.1. P4S – Politika nadzora dostopa: določa zahteve za upravljanje varnega dostopa do sistemov, vključno s sistemi, do katerih se dostopa prek mobilnih naprav. Uveljavlja higieno gesel in kontrole sej.

10.1.2. P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da so uporabniki usposobljeni za varno uporabo mobilnih naprav, poročanje o incidentih in pogoje uporabe lastnih naprav.

10.1.3. P17S – Politika varstva podatkov in zasebnosti: vzpostavlja ravnanje z osebnimi in poslovnimi podatki na mobilnih platformah v skladu z GDPR, zlasti kadar se za delo uporabljajo osebne naprave.

10.1.4. P9S – Politika dela na daljavo: usklajuje pričakovanja glede uporabe mobilnih naprav pri delu zunaj lokacije ali od doma, vključno z ravnanjem z napravami in zaščitnimi ukrepi za omrežni dostop.

10.1.5. P30S – Politika odzivanja na incidente: določa okvir odzivanja za incidente, povezane z mobilnimi napravami, vključno s kompromitiranimi ali izgubljenimi napravami.

10.2. Te povezane politike skupaj tvorijo celovit nabor kontrol za varnost mobilnih naprav v MSP brez namenskega IT-osebja ter zagotavljajo izvršljivost, preglednost in pripravljenost na certifikacijo.

11. Referenčni standardi in okviri

11.1. Ta politika podpira popolno usklajenost z naslednjimi standardi informacijske varnosti in skladnosti:

11.2. ISO/IEC 27001:

11.2.1. Klavzula 5.1 – vodenje in zavezanost: zagotavlja vodstveni nadzor in odgovornost za mobilni dostop ter uporabo lastnih naprav,

11.2.2. Klavzula 6.1 – ukrepi za obravnavo tveganj: zahteva oceno in obravnavo tveganj varnosti mobilnih naprav,

11.2.3. Klavzula 8.1 – operativno načrtovanje in nadzor: zahteva dosledne postopke mobilnega dostopa za zaščito poslovnih podatkov.

11.3. ISO/IEC 27002:

11.3.1. Kontrole 5.10 (uporaba mobilnih naprav), 5.11 (delo na daljavo), 5.12 (oddaljeni dostop) in 5.13 (uporaba lastnih naprav): podajajo smernice za upravljanje tveganj naprav v kontekstu malega podjetja.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – nadzor dostopa za mobilne naprave: zahteva varnostne nastavitve za odobreno uporabo mobilnih naprav,

11.4.2. AC-20 – uporaba zunanjih sistemov: ureja tveganja pri uporabi lastnih naprav in oddaljenem dostopu,

11.4.3. CM-6 – konfiguracijske nastavitve: uveljavlja varne privzete in prilagojene nastavitve na mobilnih platformah,

11.4.4. MP-7 – uporaba medijev: obravnava ustrezno uporabo in omejitve za mobilno shranjevanje ter dostop do podatkov.

11.5. Uredba EU GDPR (2016/679):

11.5.1. Člen 5(1)(f) – celovitost in zaupnost: zahteva varstvo podatkov z ustrezno varnostjo osebnih podatkov, zlasti na mobilnih platformah,

11.5.2. Člen 32 – varnost obdelave: nalaga uporabo ustreznih tehničnih in organizacijskih ukrepov za zaščito podatkov, do katerih se dostopa ali se hranijo na mobilnih napravah.

11.6. Direktiva EU NIS2 (2022/2555):

11.6.1. Člen 21(2)(d) – ukrepi za varnost naprav: zahteva varnostne kontrole za strojno in programsko opremo, ki se uporablja za dostop do kritičnih poslovnih sistemov, vključno z osebnimi napravami.

11.7. Uredba EU DORA (2022/2554):

11.7.1. Člen 9 – okvir upravljanja tveganj IKT: zahteva zaščito mobilnih končnih točk, ki se uporabljajo za kritične poslovne komunikacije in storitve v oblaku,

11.7.2. Člen 10 – neprekinjeno poslovanje IKT: zahteva nadaljnji varen dostop do poslovnih sistemov tudi med motnjami ali pri delu na daljavo.

11.8. COBIT 2019:

11.8.1. APO13 – upravljanje varnosti: zahteva, da organizacija uveljavi politike za mobilne naprave in uporabo lastnih naprav, usklajene s poslovnim tveganjem,

11.8.2. DSS01 – upravljanje operacij: zagotavlja tehnično izvedbo mehanizmov varnega dostopa,

11.8.3. DSS05 – upravljanje varnostnih storitev: ureja vlogo tretjih oseb pri vzdrževanju varnih mobilnih okolij in usklajevanju odziva na incidente.