					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P34					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	5.2, 6.1, 7.5, 8	Določa uporabo varnostnih kontrol in zahteve glede skladnosti
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Določa podrobne kontrole za upravljanje mobilnih naprav
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Nadzor dostopa, oddaljeni dostop, konfiguracija in varnostne zahteve za mobilne naprave
Uredba EU GDPR	5(1)(f), 25, 32	Obvezne zahteve glede zasebnosti, šifriranja podatkov in varnosti obdelave
Direktiva EU NIS2	21(2)(d)	Tehnični in organizacijski zaščitni ukrepi za mobilni dostop
Uredba EU DORA	9, 10	Upravljanje IKT-tveganj in varnostne zahteve za mobilne naprave
COBIT 2019	APO13.02, DSS01.04, BAI09	Načrti informacijske varnosti, konfiguracija sredstev in kontrole za mobilna okolja

1. Namen

1.1 Ta politika določa varnostne, skladnostne in operativne zahteve za uporabo mobilnih naprav ter osebne tehnologije v okviru uporabe lastnih naprav (BYOD – Bring Your Own Device) pri dostopu do organizacijskih sistemov, aplikacij ali podatkov.

1.2 Njen namen je zagotoviti zaupnost, celovitost in razpoložljivost (CIA) informacij podjetja, do katerih se dostopa ali se obdelujejo prek mobilnih končnih točk, vključno s pametnimi telefoni, tabličnimi računalniki, prenosniki in hibridnimi napravami.

1.3 Ta politika določa tudi tehnične in procesne kontrole, potrebne za zmanjševanje tveganj, kot so uhajanje podatkov, nepooblaščen dostop, izguba ali kraja naprave ter kompromitacija mobilnih aplikacij.

1.4 Ta politika podpira regulativno in pogodbeno skladnost ter hkrati omogoča varno mobilno produktivnost zaposlenim, pogodbenim izvajalcem in pooblaščenim tretjim osebam.

2. Področje uporabe

2.1 Ta politika velja za vse osebje, vključno z zaposlenimi, pogodbenimi izvajalci, praktikanti in ponudniki storitev tretjih oseb, ki uporabljajo mobilne naprave za dostop do podatkov podjetja, sistemov, aplikacij ali komunikacijskih platform.

2.2 Zajema vse mobilne računalniške naprave, vključno z, vendar ne omejeno na:

2.2.1 pametne telefone in tablične računalnike (iOS, Android itd.)

2.2.2 prenosnike in ultrabooke (Windows, macOS, Linux)

2.2.3 nosljive naprave in hibridne pametne naprave, ki omogočajo sinhronizacijo podatkov

2.3 Velja ne glede na to, ali je naprava v lasti podjetja ali v osebni lasti na podlagi dogovora o uporabi lastnih naprav.

2.4 Politika zajema vse načine dostopa, vključno z VPN, virtualnimi namizji, aplikacijami v oblaku, e-pošto, platformami za sodelovanje (npr. SharePoint, Teams) in orodji za sinhronizacijo datotek (npr. OneDrive, Dropbox, če je odobren).

2.5 Vključuje uporabo pri delu na daljavo, v poslovnih prostorih, na poti ali v okviru hibridnih oblik dela.

3. Cilji

3.1 Zmanjšati tveganje kompromitacije, uhajanja ali izgube podatkov zaradi nevarne uporabe mobilnih naprav.

3.2 Zagotoviti dosledne in izvršljive varnostne kontrole na vseh mobilnih končnih točkah ne glede na model lastništva (naprave podjetja ali uporaba lastnih naprav).

3.3 Zagotoviti, da je uporaba mobilnih naprav skladna z ISO/IEC 27001 in drugimi regulativnimi okviri, ki se uporabljajo za zasebnost, varstvo podatkov in kibernetsko varnost.

3.4 Omogočiti varno vključevanje mobilnih naprav v operativne, komunikacijske in sodelovalne delovne tokove organizacije.

3.5 Določiti jasno opredeljene odgovornosti in procese za upravljanje mobilnih naprav (MDM), vključno z vpisom, oddaljenim izbrisom, šifriranjem, avtentikacijo in spremljanjem.

3.6 Varovati pravice do zasebnosti posameznikov, ki uporabljajo lastne naprave, ob sočasnem varovanju občutljivih informacij organizacije.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO) / vodja varnosti IT

4.1.1 Določa politiko in tehnične standarde za uporabo mobilnih naprav in uporabo lastnih naprav.

4.1.2 Nadzoruje skladnost, odzivanje na incidente in upravljanje izjem za kontrole mobilnih naprav.

4.1.3 Delovanje usklajuje s pravno službo in kadrovsko službo (HR), da je izvajanje pravno ustrezno in organizacijsko usklajeno.

4.2 Skrbnik IT / skrbnik MDM

4.2.1 Upravlja dodelitev, vpis in konfiguracijo mobilnih naprav prek rešitev MDM.

4.2.2 Uveljavlja kontrole na ravni naprave (npr. šifriranje, kode PIN, kontrole aplikacij).

4.2.3 Po potrebi izvede oddaljeni izbris, zaklep naprave in preklic dostopa.

[... 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 To politiko mora najmanj enkrat letno pregledati vodja informacijske varnosti (CISO) ali imenovani vodja informacijske varnosti, da se zagotovi usklajenost z:

9.1.1 spremembami mobilnih platform OS, tehnologij MDM ali standardov avtentikacije,

9.1.2 regulativnimi ali pogodbenimi spremembami, ki vplivajo na varstvo mobilnih podatkov (npr. GDPR, DORA, NIS2),

9.1.3 spremembami kontrolnih sklopov ISO/IEC 27001:2022, ISO/IEC 27002:2022 ali NIST SP 800-53 Rev.5,

9.1.4 povratnimi informacijami iz presoj, pregledov po incidentu ali prijav zaposlenih.

9.2 Vmesni pregledi se lahko sprožijo zaradi:

9.2.1 varnostnih incidentov, ki vključujejo mobilne naprave ali platforme BYOD,

9.2.2 obvestila ponudnika o visoko tveganih ranljivostih v podprtih platformah,

9.2.3 uvedbe novih mobilnih aplikacij ali platform za sodelovanje, ki se uporabljajo pri poslovanju.

9.3 Posodobitve politike morajo biti:

9.3.1 dokumentirane v evidenci različic politike,

9.3.2 sporočene vsem zaposlenim in zadevnim pogodbenim izvajalcem,

9.3.3 ponovno potrjene s posodobljeno potrditvijo za vse uporabnike BYOD.

9.4 Vsi pregledi in spremembe morajo biti formalno odobreni s strani najvišjega vodstva in evidentirani v registru sprememb politike.

10. Povezane politike in povezave

10.1 Ta politika je medsebojno povezana z več ključnimi politikami v okviru sistema upravljanja informacijske varnosti (ISMS) organizacije. Pomembne povezave vključujejo:

10.1.1 P1 – Politika informacijske varnosti: določa krovna načela upravljanja za vse kontrole informacijske varnosti, vključno s tistimi, ki urejajo uporabo mobilnih naprav.

10.1.2 P3 – Politika sprejemljive uporabe (AUP): določa dopustna ravnanja in omejitve pri uporabi tehnologije, ki se neposredno uporabljajo tudi za mobilni dostop in uporabo lastnih naprav.

10.1.3 P9 – Politika dela na daljavo: določa dodatne varnostne obveznosti za mobilna delovna okolja in dopolnjuje kontrole za mobilne naprave, določene v tej politiki.

10.1.4 P13 – Politika klasifikacije in označevanja podatkov: določa, kako je treba ravnati s podatki na mobilnih napravah glede na raven klasifikacije, kar vpliva na hrambo, prenos in uveljavljanje šifriranja.

10.1.5 P22 – Politika beleženja in spremljanja: podpira zbiranje in pregled dnevnikov mobilnega dostopa za zaznavanje anomalij ali kršitev.

10.1.6 P30 – Politika odzivanja na incidente: določa, kako se obravnavajo in eskalirajo incidenti, povezani z mobilnimi napravami (npr. izguba naprave, nepooblaščen dostop).

10.1.7 P33 – Politika spremljanja presoj in skladnosti: predstavlja podlago za periodične preglede skladnosti mobilne varnosti, vključno z upoštevanjem politike uporabe lastnih naprav.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodno priznanimi okviri kibernetske varnosti in pravnimi obveznostmi, da se zagotovi varna uporaba mobilnih naprav in osebnih tehnologij v okviru uporabe lastnih naprav v podjetniških okoljih.

11.2 ISO/IEC 27001:

11.2.1 Točka 5.10 – sprejemljiva uporaba sredstev podjetja: zahteva kontrole za odgovorno uporabo sredstev podjetja, vključno z mobilnimi napravami.

11.2.2 Točka 5.11 – delo na daljavo: določa varne prakse pri dostopu do sistemov zunaj prostorov podjetja.

11.2.3 Točka 5.12 – uporaba mobilnih naprav: zahteva kontrole na podlagi tveganj za mobilne končne točke in konfiguracije BYOD.

11.2.4 Točka 5.13 – prenos informacij: zahteva zaščito informacij, prenesenih po mobilnih kanalih.

11.3 ISO/IEC 27002:2022 – kontrole 5.10 do 5.13:

11.3.1 Kontrole iz Priloge A 5.10 do 5.13 določajo, kako je treba v okviru ISMS uveljaviti mobilni dostop, šifriranje, spremljanje in zmanjševanje izgub. Te kontrole podajajo podrobna navodila za izvedbo zaščite mobilnih končnih točk, uveljavljanje kontejnerizacije, spremljanje celovitosti naprav in zagotavljanje konfiguracij BYOD, ki upoštevajo zasebnost.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – nadzor dostopa za mobilne naprave: določa osnovne zaščitne ukrepe, vključno s šifriranjem, avtentikacijo in uveljavljanjem MDM.

11.4.2 AC-17 – oddaljeni dostop: zahteva varno avtentikacijo in zaščito sej za oddaljene mobilne uporabnike.

11.4.3 CM-7 – načelo najmanjše funkcionalnosti: podpira odstranitev nepotrebnih aplikacij in funkcionalnosti z mobilnih končnih točk za zmanjšanje tveganja.

11.4.4 MP-5 – zaščita prenosa medijev: določa varen prenos podatkov iz mobilnih sistemov na zunanje cilje ali cilje v oblaku.

11.4.5 SC-12 – vzpostavitev kriptografskih ključev: zahteva uporabo varnih kriptografskih protokolov za mobilno komunikacijo in hrambo.

11.5 Uredba EU GDPR (2016/679):

11.5.1 Člen 5(1)(f) – celovitost in zaupnost: od organizacij zahteva, da osebne podatke na mobilnih napravah zaščitijo pred nepooblaščenim ali nezakonitim dostopom.

11.5.2 Člen 25 – varstvo podatkov že pri načrtovanju in privzeto varstvo podatkov: zahteva, da je zasebnost vključena v procese BYOD in MDM.

11.5.3 Člen 32 – varnost obdelave: zahteva kontrole na podlagi tveganj (npr. šifriranje, avtentikacija, nadzor dostopa) za osebne podatke na mobilnih platformah.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Člen 21(2)(d): zahteva, da je mobilni dostop do kritičnih sistemov in informacij zaščiten z ustreznimi tehničnimi in organizacijskimi ukrepi, kot so kontrola končnih točk, šifriranje in spremljanje.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Člen 9 – okvir upravljanja IKT-tveganj: zahteva, da finančni subjekti zmanjšujejo tveganja mobilnega in oddaljenega dostopa kot del operativne odpornosti.

11.7.2 Člen 10 – varnostne zahteve za sisteme IKT: zahteva varno mobilno arhitekturo, spremljanje in mehanizme odzivanja na kibernetske grožnje, ki izvirajo iz mobilnih naprav.

11.8 COBIT 2019:

11.8.1 APO13.02 – vzpostavi in vzdržuj načrt informacijske varnosti: zahteva, da je uporaba mobilnih naprav, vključno z BYOD, vključena v varnostne strategije organizacije.

11.8.2 DSS01.04 – upravljaj konfiguracijo in celovitost sredstev: uporablja se za nadzor konfiguracije in varno uvajanje mobilnih naprav.

11.8.3 BAI09.01 – vzpostavi in vzdržuj kontrole: podpira uvedbo tehničnih in procesnih varovalnih ukrepov za varno mobilno delo in oddaljene operacije.