					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P34					Naziv dokumenta: **Politika mobilnih uređaja i uporabe vlastitih uređaja (BYOD)**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Primjenjuju se sigurnosne kontrole i zahtjevi usklađenosti
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Pruža detaljne kontrole za upravljanje mobilnim uređajima
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Kontrole pristupa, udaljenog pristupa, konfiguracije i sigurnosni zahtjevi za mobilne uređaje
GDPR EU	5(1)(f), 25, 32	Obvezni zahtjevi u pogledu privatnosti, šifriranja podataka i sigurnosti obrade
Direktiva EU NIS2	21(2)(d)	Tehničke i organizacijske mjere zaštite za mobilni pristup
Uredba EU DORA	9, 10	Upravljanje IKT rizicima i sigurnosni zahtjevi za mobilne uređaje
COBIT 2019	APO13.02, DSS01.04, BAI09	Planovi informacijske sigurnosti, konfiguracija imovine i kontrole za mobilna okruženja

1. Svrha

1.1 Ova politika utvrđuje sigurnosne, usklađenosne i operativne zahtjeve za uporabu mobilnih uređaja i vlastitih uređaja (BYOD) pri pristupu organizacijskim sustavima, aplikacijama ili podacima.

1.2 Cilj ove politike je osigurati povjerljivost, cjelovitost i dostupnost informacija društva kojima se pristupa ili koje se obrađuju putem mobilnih krajnjih uređaja, uključujući pametne telefone, tablete, prijenosna računala i hibridne uređaje.

1.3 Ova politika također propisuje tehničke i postupovne kontrole potrebne za ublažavanje rizika kao što su curenje podataka, neovlašteni pristup, gubitak ili krađa uređaja te kompromitacija mobilnih aplikacija.

1.4 Ova politika podupire usklađenost s regulatornim i ugovornim zahtjevima te istodobno omogućuje sigurnu mobilnu produktivnost zaposlenicima, ugovornim izvođačima i ovlaštenim trećim stranama.

2. Područje primjene

2.1 Ova politika primjenjuje se na cjelokupno osoblje, uključujući zaposlenike, ugovorne izvođače, vježbenike i pružatelje usluga trećih strana, koji upotrebljavaju mobilne uređaje za pristup podacima, sustavima, aplikacijama ili komunikacijskim platformama društva.

2.2 Obuhvaća sve mobilne računalne uređaje, uključujući, ali ne ograničavajući se na:

2.2.1 pametne telefone i tablete (iOS, Android i dr.)

2.2.2 prijenosna računala i ultrabook uređaje (Windows, macOS, Linux)

2.2.3 nosive uređaje i hibridne pametne uređaje sposobne za sinkronizaciju podataka

2.3 Primjenjuje se neovisno o tome je li uređaj u vlasništvu društva ili je riječ o privatnom uređaju (BYOD) na temelju odgovarajućeg sporazuma.

2.4 Politika obuhvaća sve načine pristupa, uključujući VPN, virtualne radne površine, aplikacije u oblaku, e-poštu, platforme za suradnju (npr. SharePoint, Teams) i alate za sinkronizaciju datoteka (npr. OneDrive, Dropbox ako je odobren).

2.5 Uključuje uporabu pri radu na daljinu, u prostorijama društva, tijekom putovanja ili u hibridnim oblicima rada.

3. Ciljevi

3.1 Smanjiti rizik od kompromitacije, curenja ili gubitka podataka zbog nesigurne uporabe mobilnih uređaja.

3.2 Osigurati dosljednu i provedivu primjenu sigurnosnih kontrola na svim mobilnim krajnjim uređajima, neovisno o modelu vlasništva (organizacijski ili BYOD).

3.3 Osigurati da je uporaba mobilnih uređaja usklađena s normom ISO/IEC 27001 i drugim regulatornim okvirima primjenjivima na privatnost, zaštitu podataka i kibernetičku sigurnost.

3.4 Omogućiti sigurnu integraciju mobilnih uređaja u operativne, komunikacijske i suradničke tijekove rada organizacije.

3.5 Uspostaviti jasno definirane odgovornosti i procese za upravljanje mobilnim uređajima (MDM), uključujući upis uređaja, udaljeno brisanje podataka, šifriranje, autentifikaciju i nadzor.

3.6 Zaštititi prava privatnosti pojedinaca koji upotrebljavaju vlastite uređaje, uz istodobnu zaštitu osjetljivih informacija organizacije.

4. Uloge i odgovornosti

4.1 Glavni službenik za informacijsku sigurnost (CISO) / voditelj informacijske sigurnosti

4.1.1 Definira politiku i tehničke standarde za uporabu mobilnih uređaja i BYOD-a.

4.1.2 Nadzire usklađenost, odgovor na incidente i upravljanje iznimkama za kontrole mobilnih uređaja.

4.1.3 Koordinira s timovima za ljudske resurse i pravne poslove kako bi osigurao da je provedba pravno utemeljena i usklađena s organizacijskim zahtjevima.

4.2 IT administrator / administrator MDM-a

4.2.1 Upravlja dodjelom, upisom i konfiguracijom mobilnih uređaja putem MDM rješenja.

4.2.2 Provodi kontrole na razini uređaja (npr. šifriranje, PIN-ove, kontrole aplikacija).

4.2.3 Provodi udaljeno brisanje podataka, zaključavanje uređaja i ukidanje prava pristupa kada je to potrebno.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1 Ovu politiku mora pregledati najmanje jednom godišnje CISO ili imenovani voditelj informacijske sigurnosti kako bi se osigurala usklađenost sa:

9.1.1 promjenama platformi mobilnih operativnih sustava, MDM tehnologija ili standarda autentifikacije

9.1.2 regulatornim ili ugovornim promjenama koje utječu na zaštitu mobilnih podataka (npr. GDPR, DORA, NIS2)

9.1.3 izmjenama skupova kontrola ISO/IEC 27001:2022, ISO/IEC 27002:2022 ili NIST SP 800-53 Rev.5

9.1.4 povratnim informacijama iz revizija, naknadnih analiza incidenata ili prijava zaposlenika

9.2 Izvanredni pregledi mogu se pokrenuti zbog:

9.2.1 sigurnosnih incidenata koji uključuju mobilne uređaje ili BYOD platforme

9.2.2 obavijesti dobavljača o ranjivostima visokog rizika na podržanim platformama

9.2.3 uvođenja novih mobilnih aplikacija ili platformi za suradnju koje se upotrebljavaju za poslovne operacije

9.3 Ažuriranja politike moraju biti:

9.3.1 dokumentirana u povijesti verzija politike

9.3.2 priopćena cjelokupnom osoblju i pogođenim ugovornim izvođačima

9.3.3 ponovno potvrđena ažuriranom potvrdom upoznatosti za sve BYOD korisnike

9.4 Svi pregledi i izmjene moraju biti formalno odobreni od strane izvršnog rukovodstva i evidentirani u registru promjena politike.

10. Povezane politike i poveznice

10.1 Ova je politika međuovisna s nekoliko ključnih politika u okviru sustava upravljanja informacijskom sigurnošću organizacije. Važne poveznice uključuju:

10.1.1 P1 – Politika informacijske sigurnosti: utvrđuje krovna načela upravljanja za sve kontrole informacijske sigurnosti, uključujući one koje uređuju uporabu mobilnih uređaja.

10.1.2 P3 – Politika prihvatljive uporabe: definira dopuštena ponašanja i ograničenja povezana s uporabom tehnologije, koja se izravno primjenjuju na mobilni i BYOD pristup.

10.1.3 P9 – Politika rada na daljinu: uređuje dodatne sigurnosne obveze za mobilna radna okruženja i nadopunjuje kontrole specifične za mobilne uređaje definirane ovom politikom.

10.1.4 P13 – Politika klasifikacije podataka i označavanja: uređuje postupanje s podacima na mobilnim uređajima prema razini klasifikacije, što utječe na pohranu, prijenos i provedbu šifriranja.

10.1.5 P22 – Politika zapisivanja događaja i praćenja: podupire prikupljanje i pregled evidencije mobilnog pristupa radi otkrivanja anomalija ili kršenja.

10.1.6 P30 – Politika odgovora na incidente: uređuje način postupanja s incidentima povezanima s mobilnim uređajima (npr. gubitak uređaja, neovlašteni pristup) i njihovu eskalaciju.

10.1.7 P33 – Politika revizijskog praćenja i usklađenosti: pruža osnovu za periodične provjere usklađenosti sigurnosti mobilnih uređaja, uključujući pridržavanje BYOD politike.

11. Referentni standardi i okviri

11.1 Ova je politika usklađena s međunarodno priznatim okvirima kibernetičke sigurnosti i pravnim obvezama kako bi se osigurala sigurna uporaba mobilnih uređaja i vlastitih uređaja (BYOD) u poslovnim okruženjima.

11.2 ISO/IEC 27001:

11.2.1 Točka 5.10 – Prihvatljiva uporaba imovine organizacije: zahtijeva kontrole za odgovornu uporabu korporativne imovine, uključujući mobilne uređaje.

11.2.2 Točka 5.11 – Rad na daljinu: uređuje sigurne prakse pri pristupu sustavima izvan prostora društva.

11.2.3 Točka 5.12 – Uporaba mobilnih uređaja: propisuje kontrole temeljene na riziku za mobilne krajnje uređaje i BYOD konfiguracije.

11.2.4 Točka 5.13 – Prijenos informacija: nalaže zaštitu informacija koje se prenose putem mobilnih kanala.

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

11.3.1 Kontrole iz Priloga A 5.10 do 5.13 određuju kako se unutar ISMS-a moraju provoditi mobilni pristup, šifriranje, praćenje i ublažavanje gubitka. Te kontrole pružaju detaljne smjernice za provedbu zaštite mobilnih krajnjih uređaja, provedbu kontejnerizacije, praćenje cjelovitosti uređaja i osiguravanje konfiguracija BYOD uporabe koje uvažavaju privatnost.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Kontrola pristupa za mobilne uređaje: definira osnovne zaštitne mjere, uključujući šifriranje, autentifikaciju i provedbu MDM-a.

11.4.2 AC-17 – Udaljeni pristup: zahtijeva sigurnu autentifikaciju i zaštitu sesija za udaljene mobilne korisnike.

11.4.3 CM-7 – Minimalna funkcionalnost: podupire uklanjanje nepotrebnih aplikacija i funkcionalnosti s mobilnih krajnjih uređaja radi smanjenja rizika.

11.4.4 MP-5 – Zaštita prijenosa medija: uređuje siguran prijenos podataka iz mobilnih sustava prema vanjskim odredištima ili odredištima u oblaku.

11.4.5 SC-12 – Uspostava kriptografskih ključeva: nalaže uporabu sigurnih kriptografskih protokola za mobilnu komunikaciju i pohranu.

11.5 GDPR EU (2016/679):

11.5.1 Članak 5(1)(f) – Cjelovitost i povjerljivost: zahtijeva da organizacije zaštite osobne podatke na mobilnim uređajima od neovlaštenog ili nezakonitog pristupa.

11.5.2 Članak 25 – Zaštita podataka u fazi projektiranja i prema zadanim postavkama: zahtijeva da privatnost bude ugrađena u BYOD i MDM procese.

11.5.3 Članak 32 – Sigurnost obrade: nalaže kontrole temeljene na riziku (npr. šifriranje, autentifikacija, kontrola pristupa) za osobne podatke na mobilnim platformama.

11.6 Direktiva EU NIS2 (2022/2555):

11.6.1 Članak 21(2)(d): nalaže da mobilni pristup kritičnim sustavima i informacijama bude zaštićen odgovarajućim tehničkim i organizacijskim mjerama, kao što su kontrola krajnjih uređaja, šifriranje i praćenje.

11.7 Uredba EU DORA (2022/2554):

11.7.1 Članak 9 – Okvir za upravljanje IKT rizicima: zahtijeva da subjekti u financijskom sektoru ublažavaju rizike mobilnog i udaljenog pristupa kao dio operativne otpornosti.

11.7.2 Članak 10 – Zahtjevi sigurnosti IKT sustava: zahtijeva sigurnu mobilnu arhitekturu, praćenje i mehanizme odgovora na kibernetičke prijetnje koje potječu s mobilnih uređaja.

11.8 COBIT 2019:

11.8.1 APO13.02 – Uspostaviti i održavati plan informacijske sigurnosti: zahtijeva da uporaba mobilnih uređaja, uključujući BYOD, bude integrirana u organizacijske sigurnosne strategije.

11.8.2 DSS01.04 – Upravljati konfiguracijom i cjelovitošću imovine: primjenjuje se na kontrolu konfiguracije i sigurno uvođenje mobilnih uređaja.

11.8.3 BAI09.01 – Uspostaviti i održavati kontrole: podupire provedbu tehničkih i postupovnih zaštitnih mjera za sigurne mobilne i udaljene operacije.