					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P34S					Naziv dokumenta: **Politika mobilnih uređaja i korištenja 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 regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 5.1, 5.2, 6.1, 6.2, 8	Opći zahtjevi za ISMS i kontrole za mobilne uređaje/BYOD
ISO/IEC 27002:2022	Kontrole 5.10–5.13	Detaljne kontrole za mobilne uređaje/BYOD i udaljeni pristup
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Federalne kontrole za uređaje, medije i konfiguraciju
EU GDPR	Članak 5(1)(f)	Zaštita osobnih podataka na mobilnim krajnjim uređajima
EU NIS2	Članak 21(2)(d)	Zaštita poslovno kritičnih uređaja, uključujući BYOD
EU DORA	Članci 9, 10	IKT rizik i kontinuitet poslovanja za mobilne krajnje uređaje
COBIT 2019	APO13, DSS01, DSS05	Upravljanje IT-jem, operacijama i kontrolama sigurnosnih usluga

1. Svrha

1.1. Ova politika utvrđuje obvezne sigurnosne zahtjeve za uporabu mobilnih uređaja, uključujući pametne telefone, tablete i prijenosna računala, pri pristupu informacijama, sustavima ili uslugama organizacije.

1.2. Ova politika također uređuje korištenje vlastitih uređaja (BYOD) radi osiguranja zaštite podataka klijenata i poslovnih podataka, neovisno o vlasništvu nad uređajem.

1.3. Ova politika osigurava dosljednu zaštitu mobilnog pristupa, podupire ciljeve certifikacije prema normi ISO/IEC 27001 te sprječava gubitak podataka ili kompromitaciju uslijed gubitka, krađe ili nepravilne uporabe mobilnih krajnjih uređaja.

1.4. Ova politika osigurava primjenu tehničkih i organizacijskih mjera na uporabu mobilnih uređaja u SME organizacijama bez namjenskih IT timova, uključujući rad na daljinu i usluge u oblaku.

2. Područje primjene

2.1. Ova politika primjenjuje se na sve zaposlenike, ugovorne izvođače, vježbenike i pružatelje usluga koji:

2.1.1. koriste mobilni uređaj za pristup, obradu ili pohranu podataka ili sustava organizacije

2.1.2. povezuju se na usluge organizacije, uključujući e-poštu, zajedničke mape, aplikacije u oblaku ili interne sustave putem VPN-a

2.2. Ova politika obuhvaća:

2.2.1. sve mobilne uređaje: pametne telefone, tablete i prijenosna računala (u vlasništvu organizacije ili privatne uređaje (BYOD))

2.2.2. sve operacijske sustave (npr. iOS, Android, Windows, macOS)

2.2.3. sve lokacije (ured, dom, udaljene lokacije, javni prostori)

2.3. Ova politika primjenjuje se u svim radnim okruženjima i mora se provoditi neovisno o vlasništvu nad uređajem.

3. Ciljevi

3.1. Sprječavanje gubitka podataka: osigurati da uporaba mobilnih uređaja ne izlaže osjetljive podatke organizacije ili klijenata neovlaštenom pristupu, krađi ili zlouporabi.

3.2. Definiranje jasnih pravila za BYOD: propisati provedive uvjete za uporabu privatnih uređaja u poslovne svrhe, uz odgovarajuće pravne i tehničke zaštitne mjere.

3.3. Podrška regulatornoj usklađenosti: ispuniti zahtjeve normi ISO/IEC 27001, GDPR-a, NIS2 i drugih pravnih obveza primjenom provedivih praksi sigurnosti mobilnih uređaja.

3.4. Smanjenje operativnog rizika: smanjiti vjerojatnost operativnih poremećaja uzrokovanih zlouporabom, kompromitacijom ili neispravnošću mobilnih uređaja.

3.5. Očuvanje povjerenja klijenata: dokazati klijentima i partnerima da su njihovi podaci zaštićeni i kada im se pristupa s mobilnih ili privatnih uređaja.

4. Uloge i odgovornosti

4.1. glavni direktor (GM):

4.1.1. zadržava odgovornost za ovu politiku.

4.1.2. odobrava svu uporabu mobilnog pristupa i BYOD pristupa sustavima organizacije.

4.1.3. osigurava da su BYOD sporazumi potpisani, pohranjeni i pod nadzorom.

4.1.4. provjerava da vanjski pružatelji IT usluga provode propisane zaštitne mjere za mobilne uređaje.

4.2. Imenovano osoblje ili IT podrška:

4.2.1. pruža podršku pri postavljanju, registraciji i konfiguraciji mobilnih uređaja koji se koriste za rad.

4.2.2. provodi kontrole pristupa, ograničenja aplikacija i politike nadzora povezane s mobilnim uređajima.

4.2.3. pruža podršku u odgovoru na incidente povezane s mobilnim uređajima (izgubljeni, ukradeni ili kompromitirani uređaji).

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

9. Zahtjevi za pregled i ažuriranje

9.1. Godišnji pregled

9.1.1. glavni direktor (GM) mora pregledati ovu politiku najmanje jednom u 12 mjeseci.

9.1.2. pregled mora potvrditi trajnu usklađenost sa zahtjevima norme ISO/IEC 27001, razvojem mobilnih tehnologija i promjenama u poslovanju.

9.1.3. ažuriranja moraju uzeti u obzir i nedavne incidente, rezultate revizije ili regulatorne promjene (npr. GDPR, NIS2, DORA).

9.2. Pokretači izvanrednog pregleda

9.2.1. ova politika mora se bez odgode ažurirati ako nastupi bilo koja od sljedećih okolnosti:

9.2.1.1. veći sigurnosni incident povezan s mobilnim uređajima (npr. povreda putem izgubljenog ili kompromitiranog uređaja)

9.2.1.2. promjena podržanih platformi ili alata za upravljanje mobilnim uređajima

9.2.1.3. pravna ili regulatorna promjena koja utječe na uporabu privatnih uređaja ili zaštitu podataka

9.2.1.4. uvođenje novih aplikacija, usluga ili alata trećih strana koji se koriste na mobilnim uređajima

9.3. Dokumentiranje promjena

9.3.1. svi pregledi i ažuriranja moraju biti dokumentirani, uključujući datum pregleda, unesene promjene i odobrenje GM-a

9.3.2. povijest verzija mora se zadržati za potrebe revizije

9.4. Komunikacija i pristup

9.4.1. GM mora osigurati da su svi korisnici (zaposlenici, ugovorni izvođači, treće strane) obaviješteni o promjenama

9.4.2. ažurirane verzije moraju biti lako dostupne, primjerice u zajedničkim mapama ili na internim platformama

10. Povezane politike i poveznice

10.1. Ova politika čini dio ukupnog skupa SME politika informacijske sigurnosti i mora se provoditi zajedno sa sljedećim dokumentima:

10.1.1. P4S – Politika kontrole pristupa: definira zahtjeve za upravljanje sigurnim pristupom sustavima, uključujući pristup putem mobilnih uređaja. Propisuje higijenu lozinki i kontrole sesija.

10.1.2. P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da su korisnici osposobljeni za sigurnu uporabu mobilnih uređaja, prijavljivanje incidenata i BYOD uvjete.

10.1.3. P17S – Politika zaštite podataka i privatnosti: uspostavlja postupanje s osobnim i poslovnim podacima na mobilnim platformama u skladu s GDPR-om, osobito kada se za rad koriste privatni uređaji.

10.1.4. P9S – Politika rada na daljinu: usklađuje očekivanja za uporabu mobilnih uređaja pri radu izvan lokacije ili od kuće, uključujući postupanje s uređajima i zaštitne mjere mrežnog pristupa.

10.1.5. P30S – Politika odgovora na incidente: pruža okvir za odgovor na incidente povezane s mobilnim uređajima, uključujući kompromitirane ili izgubljene uređaje.

10.2. Ove povezane politike zajedno čine cjelovit skup kontrola za sigurnost mobilnih uređaja u SME organizacijama bez namjenskog IT osoblja te osiguravaju provedivost, transparentnost i spremnost za certifikaciju.

11. Referentni standardi i okviri

11.1. Ova politika podupire punu usklađenost sa sljedećim standardima sigurnosti i usklađenosti:

11.2. ISO/IEC 27001:

11.2.1. Točka 5.1 – Vodstvo i opredijeljenost: osigurava nadzor uprave i odgovornost za mobilni pristup i BYOD

11.2.2. Točka 6.1 – Radnje za postupanje s rizicima: zahtijeva procjenu i obradu rizika sigurnosti mobilnih uređaja

11.2.3. Točka 8.1 – Operativno planiranje i kontrola: zahtijeva dosljedne postupke mobilnog pristupa radi zaštite poslovnih podataka

11.3. ISO/IEC 27002:

11.3.1. Kontrole 5.10 (uporaba mobilnih uređaja), 5.11 (rad na daljinu), 5.12 (udaljeni pristup) i 5.13 (BYOD): daju smjernice za provedbu upravljanja rizicima uređaja u kontekstu malog poslovnog sustava

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – kontrola pristupa za mobilne uređaje: zahtijeva sigurnosne postavke za odobrenu uporabu mobilnih uređaja

11.4.2. AC-20 – uporaba vanjskih sustava: uređuje rizike BYOD-a i udaljenog pristupa

11.4.3. CM-6 – postavke konfiguracije: propisuje sigurne zadane i prilagođene postavke na mobilnim platformama

11.4.4. MP-7 – uporaba medija: uređuje pravilnu uporabu i ograničenja za mobilnu pohranu i pristup podacima

11.5. GDPR EU (2016/679):

11.5.1. Članak 5(1)(f) – cjelovitost i povjerljivost: zahtijeva zaštitu podataka odgovarajućom sigurnošću osobnih podataka, osobito na mobilnim platformama

11.5.2. Članak 32 – sigurnost obrade: obvezuje na primjenu odgovarajućih tehničkih i organizacijskih mjera za zaštitu podataka kojima se pristupa ili koji se pohranjuju na mobilnim uređajima

11.6. Direktiva NIS2 EU (2022/2555):

11.6.1. Članak 21(2)(d) – mjere sigurnosti uređaja: zahtijeva sigurnosne kontrole za hardver i softver koji se koriste za pristup kritičnim poslovnim sustavima, uključujući privatne uređaje

11.7. Uredba DORA EU (2022/2554):

11.7.1. Članak 9 – okvir za upravljanje IKT rizicima: zahtijeva zaštitu mobilnih krajnjih uređaja koji se koriste za kritične poslovne komunikacije i usluge u oblaku

11.7.2. Članak 10 – IKT kontinuitet poslovanja: zahtijeva neprekinut siguran pristup poslovnim sustavima i tijekom poremećaja ili rada na daljinu

11.8. COBIT 2019:

11.8.1. APO13 – Upravljanje sigurnošću: zahtijeva da organizacija provodi politike za mobilne uređaje i BYOD usklađene s poslovnim rizikom

11.8.2. DSS01 – Upravljanje operacijama: osigurava tehničku provedbu mehanizama sigurnog pristupa

11.8.3. DSS05 – Upravljanje sigurnosnim uslugama: uređuje uključenost trećih strana u održavanje sigurnih mobilnih okruženja i koordinaciju odgovora na incidente