					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P29S					Naslov dokumenta: **Politika testnih podatkov in testnih okolij**							
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	Klavzuli 6.1, 8	
ISO/IEC 27002:2022	Kontroli 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
Uredba (EU) GDPR	Členi 5(1)(c), 25, 32	
Direktiva (EU) NIS2	Člen 21(2)(e), (h)	
Uredba (EU) DORA	Člen 9	
COBIT 2019	BAI07, DSS05	

1. Namen

1.1 Ta politika določa način upravljanja testnih podatkov in testnih okolij, da se med testiranjem preprečijo nenamerna razkritja, kršitve varnosti osebnih podatkov in operativne motnje.

1.2 Zagotavlja, da se resnični podatki o strankah pri testiranju programske opreme ali sistemov nikoli ne uporabljajo neustrezno ter da so testna okolja logično in tehnično ločena od produkcijskih sistemov.

1.3 Politika je zasnovana tako, da MSP podpira pri izpolnjevanju zahtev za certifikacijo ISO/IEC 27001 in veljavne zakonodaje s področja varstva podatkov, pri čemer ostaja praktična in izvedljiva tudi za organizacije brez namenske IT-ekipe.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vsa testna okolja (npr. pripravljalni strežniki, peskovniki, razvojna testna okolja),

2.1.2 vse testne podatke, ne glede na to, ali so ročno ustvarjeni, generirani ali izpeljani iz produkcijskih podatkov,

2.1.3 vse osebe, vključene v testne dejavnosti, vključno z zaposlenimi, pogodbenimi izvajalci, samostojnimi izvajalci in ponudniki IT-storitev,

2.1.4 vsako testiranje, ki bi lahko vplivalo na platforme, dostopne strankam, interne poslovne sisteme ali storitve tretjih oseb.

2.2 Politika zajema tehnična okolja in procese, ki se uporabljajo za podporo:

2.2.1 razvoju spletnih mest, aplikacij in orodij,

2.2.2 nadgradnjam sistemov, testiranju konfiguracij in integracijskemu testiranju,

2.2.3 avtomatiziranemu in ročnemu funkcionalnemu ali varnostnemu testiranju.

3. Cilji

3.1 Preprečiti uporabo resničnih, prepoznavnih podatkov o strankah pri testiranju, razen če so anonimizirani in izrecno odobreni.

3.2 Ohranjati strogo ločitev med testnimi in produkcijskimi sistemi, da se preprečita nenamerna izpostavljenost podatkov in operativno poseganje.

3.3 Zaščititi testne sisteme in podatke pred nepooblaščenim dostopom, nenamernim razkritjem ali ponovno uporabo med okolji brez ustreznih kontrol.

3.4 Zagotoviti skladnost z veljavnimi predpisi o varstvu podatkov (npr. GDPR, NIS2) tako, da se vsi testni podatki obdelujejo zakonito, pošteno in varno.

3.5 Podpreti pripravljenost organizacije na zunanje presoje in certifikacijo ISO/IEC 27001 z dokumentiranjem praks testiranja in doslednim izvajanjem varovalnih ukrepov.

4. Vloge in odgovornosti

4.1 Generalni direktor (GM)

4.1.1 Nosi splošno odgovornost za varstvo testnih podatkov in varnost testnih sistemov.

4.1.2 Odobri vsako uporabo resničnih podatkov pri testiranju po potrditvi, da so vzpostavljeni ustrezni varovalni ukrepi (npr. anonimizacija ali maskiranje podatkov).

4.1.3 Preveri, da so testne dejavnosti ustrezno dokumentirane in skladne s to politiko.

4.2 Vodja projekta

4.2.1 Koordinira načrtovanje in izvedbo procesov testiranja.

4.2.2 Zagotovi, da vsi člani ekipe razumejo in upoštevajo to politiko.

4.2.3 Potrdi, da so testni sistemi pred začetkom testiranja varno konfigurirani.

4.2.4 O vseh incidentih, povezanih s testnimi okolji ali uhajanjem podatkov, poroča GM.

[... 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 Načrtovani pregledi

9.1.1 To politiko mora najmanj enkrat letno pregledati generalni direktor (GM). Namen pregleda je zagotoviti, da politika ostaja ažurna glede na:

9.1.1.1 spremembe v orodjih, platformah ali okoljih za razvoj programske opreme,

9.1.1.2 posodobljene pravne obveznosti, vključno z zahtevami glede varstva podatkov ali digitalne odpornosti,

9.1.1.3 certifikacijo MSP in pripravljenost na revizijo v skladu z ISO/IEC 27001.

9.2 Sprožilni dogodki za vmesni pregled

9.2.1 Dodatni pregledi se morajo izvesti po:

9.2.1.1 vsakem incidentu, ki vključuje izpostavljenost podatkov ali kompromitacijo v testnih okoljih,

9.2.1.2 uporabi resničnih podatkov pri testiranju, tudi če so anonimizirani,

9.2.1.3 uvedbi novih metod testiranja, sistemov ali dobaviteljev,

9.2.1.4 regulatornih spremembah, ki vplivajo na ravnanje s podatki med testiranjem.

9.3 Upravljanje sprememb in komunikacija

9.3.1 GM je odgovoren za:

9.3.1.1 posodabljanje te politike in dokumentiranje vseh sprememb z evidenco različic,

9.3.1.2 obveščanje zaposlenih, razvijalcev in relevantnih ponudnikov storitev o posodobitvah,

9.3.1.3 potrditev, da vse osebe, vključene v testiranje, razumejo in uporabljajo najnovejša pravila,

9.3.1.4 vzdrževanje dostopne različice veljavne politike za potrebe pregleda in revizije.

9.4 Revizija in dokumentacija

9.4.1 Evidence o vseh pregledih politike, odobritvah uporabe resničnih podatkov in vseh utemeljitvah izjem morajo biti:

9.4.1.1 varno hranjene za namene revizije,

9.4.1.2 na voljo na zahtevo med notranjimi revizijami ali revizijami tretjih oseb,

9.4.1.3 letno pregledane, da se zagotovi skladnost s praksami testiranja.

10. Povezane politike in povezave

10.1 To politiko je treba uporabljati usklajeno z naslednjimi politikami SME, da se med testiranjem ohranjata varnost in skladnost:

10.1.1 P2S – Politika vlog in odgovornosti upravljanja: določa, kdo je odgovoren za nadzor razvoja, testiranja in odgovornosti glede ločevanja sistemov.

10.1.2 P4S – Politika nadzora dostopa: ureja dodeljevanje, upravljanje in ukinitev poverilnic za dostop do testnih sistemov.

10.1.3 P8S – Politika ozaveščanja in usposabljanja na področju informacijske varnosti: zagotavlja, da zaposleni razumejo tveganja testnih podatkov, prakse varnega ravnanja in ustrezno ločevanje okolij.

10.1.4 P13S – Politika klasifikacije in označevanja podatkov: podpira jasno razvrščanje testnih podatkov in usmerja strategije anonimizacije ali maskiranja podatkov.

10.1.5 P17S – Politika varstva podatkov in zasebnosti: usklajuje obveznosti po GDPR, vključno z varovalnimi ukrepi pri obdelavi in hrambi osebnih podatkov, tudi v testnih okoljih.

10.1.6 P24S – Politika varnega razvoja: določa splošna varnostna pričakovanja za razvojne ekipe, vključno z varno uporabo podatkov v fazah testiranja.

10.1.7 P30S – Politika odzivanja na incidente: določa, kako se odzvati na vsako kršitev ali težavo, odkrito v testnem okolju ali povzročeno z neustreznim ravnanjem s testnimi podatki.

10.2 Te politike tvorijo enoten okvir informacijske varnosti za podporo celovitosti testiranja, minimizaciji podatkov in popolni skladnosti z ISO/IEC 27001 v razvojnih dejavnostih in dejavnostih zagotavljanja kakovosti.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.1 – zahteva oceno tveganja in ukrepe za obravnavo tveganj, vključno s tveganji, povezanimi s testiranjem.

11.1.2 Klavzula 8.1 – zahteva načrtovanje in nadzor operativnih procesov, vključno z vzpostavitvijo okolij testnih sistemov.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.28 – zahteva, da organizacije zaščitijo testne podatke in zagotovijo, da ti ne vsebujejo občutljivih ali produkcijskih podatkov.

11.2.2 Kontrola 8.29 – zahteva jasno ločitev razvojnih, testnih in produkcijskih okolij.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – zajema pričakovanja glede kontrol razvoja in testiranja.

11.3.2 SA-12 – obravnava tveganja testiranja v dobavni verigi in varnostna vrednotenja.

11.3.3 SC-32 – zahteva ločitev okolij ter zaščito zaupnosti in celovitosti testnih podatkov.

11.4 Splošna uredba EU o varstvu podatkov (GDPR)

11.4.1 Člen 5(1)(c) – zahteva minimizacijo podatkov, vključno z uporabo samo nujno potrebnih podatkov za testiranje.

11.4.2 Člen 25 – zahteva varstvo podatkov že pri načrtovanju, kar vključuje tudi kontrole testnih okolij.

11.4.3 Člen 32 – zahteva varno obdelavo osebnih podatkov v vseh sistemih, vključno z neprodukcijskimi okolji.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(e, h) – zahteva varen razvoj in testiranje sistemov, zlasti kadar so digitalne storitve izpostavljene kibernetskim tveganjem.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 9 – poudarja pomen digitalne operativne odpornosti, vključno z varnim testiranjem sistemov IKT v MSP iz finančnega sektorja.

11.7 COBIT 2019

11.7.1 BAI07 – Upravljanje sprejema sprememb in prehoda: vključuje kontrole testiranja za validacijo novih sistemov in ravnanja s podatki.

11.7.2 DSS05 – Upravljanje varnostnih storitev: zahteva testne in razvojne prakse, ki preprečujejo neustrezno uporabo ali izpostavljenost poslovnih podatkov.