					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P29S					Naziv dokumenta: **Politika testnih podataka i testnih okruženja**							
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 6.1, 8	
ISO/IEC 27002:2022	Kontrole 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
GDPR EU	Članci 5(1)(c), 25, 32	
Direktiva EU NIS2	Članak 21(2)(e), (h)	
Uredba EU DORA	Članak 9	
COBIT 2019	BAI07, DSS05	

1. Svrha

1.1 Ova politika definira način upravljanja testnim podacima i testnim okruženjima radi sprječavanja slučajnog izlaganja podataka, povreda podataka i operativnih poremećaja tijekom aktivnosti testiranja.

1.2 Ovom politikom osigurava se da se stvarni podaci klijenata nikada ne koriste neprimjereno tijekom testiranja softvera ili sustava te da su testna okruženja logički i tehnički odvojena od produkcijskih sustava.

1.3 Politika je izrađena kako bi pomogla SME organizacijama u ispunjavanju zahtjeva za certifikaciju prema ISO/IEC 27001 i primjenjivim propisima o zaštiti podataka, uz zadržavanje praktične primjenjivosti i provedivosti u organizacijama bez namjenskog IT tima.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 sva testna okruženja (npr. pripremni poslužitelji, sandbox sustavi, razvojna testna okruženja)

2.1.2 sve testne podatke, neovisno o tome jesu li ručno izrađeni, generirani ili izvedeni iz produkcijskih podataka

2.1.3 svo osoblje uključeno u aktivnosti testiranja, uključujući zaposlenike, ugovorne izvođače, freelancere i pružatelje IT usluga

2.1.4 svako testiranje koje može utjecati na platforme dostupne klijentima, interne poslovne sustave ili usluge trećih strana

2.2 Obuhvaća i tehnička okruženja i procese koji se koriste kao podrška za:

2.2.1 razvoj internetskih stranica, aplikacija i alata

2.2.2 nadogradnje sustava, testiranje konfiguracija i integracijsko testiranje

2.2.3 automatizirano i ručno funkcionalno ili sigurnosno testiranje

3. Ciljevi

3.1 Spriječiti uporabu stvarnih, prepoznatljivih podataka klijenata u testiranju, osim ako su anonimizirani i izričito odobreni.

3.2 Održavati strogu odvojenost između testnih i produkcijskih sustava kako bi se izbjeglo nenamjerno izlaganje podataka ili operativni poremećaji.

3.3 Zaštititi testne sustave i podatke od neovlaštenog pristupa, slučajnog otkrivanja ili ponovne uporabe među okruženjima bez odgovarajućih kontrola.

3.4 Postupati u skladu s relevantnim propisima o zaštiti podataka (npr. GDPR, NIS2) tako da se svi testni podaci obrađuju zakonito, pošteno i sigurno.

3.5 Poduprijeti spremnost organizacije za vanjske revizije i certifikaciju prema ISO/IEC 27001 dokumentiranjem praksi testiranja i provedbom dosljednih zaštitnih mjera.

4. Uloge i odgovornosti

4.1 glavni direktor (GM)

4.1.1 Ima ukupnu odgovornost za zaštitu testnih podataka i sigurnost testnih sustava.

4.1.2 Odobrava svaku uporabu stvarnih podataka u testiranju nakon potvrde da su primijenjene odgovarajuće zaštitne mjere (npr. anonimizacija ili maskiranje podataka).

4.1.3 Provjerava jesu li aktivnosti testiranja pravilno dokumentirane i usklađene s ovom politikom.

4.2 voditelj projekta

4.2.1 Koordinira osmišljavanje i provedbu procesa testiranja.

4.2.2 Osigurava da svi članovi tima razumiju i primjenjuju ovu politiku.

4.2.3 Potvrđuje da su testni sustavi sigurno konfigurirani prije početka testiranja.

4.2.4 Prijavljuje GM-u sve incidente povezane s testnim okruženjima ili curenjem podataka.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Planirani pregledi

9.1.1 Ovu politiku mora najmanje jednom godišnje pregledati glavni direktor (GM). Pregledom se osigurava da politika ostane ažurna u odnosu na:

9.1.1.1 promjene u alatima, platformama ili okruženjima za razvoj softvera

9.1.1.2 ažurirane pravne obveze, uključujući zahtjeve u području zaštite podataka ili digitalne otpornosti

9.1.1.3 certifikaciju SME organizacije i spremnost za reviziju prema ISO/IEC 27001

9.2 Pokretači izvanrednog pregleda

9.2.1 Dodatni pregledi moraju se provesti nakon:

9.2.1.1 svakog incidenta koji uključuje izlaganje podataka ili kompromitaciju u testnim okruženjima

9.2.1.2 uporabe stvarnih podataka u testiranju, čak i ako su anonimizirani

9.2.1.3 uvođenja novih metoda testiranja, sustava ili dobavljača

9.2.1.4 regulatornih promjena koje utječu na postupanje s podacima tijekom testiranja

9.3 Upravljanje promjenama i komunikacija

9.3.1 GM je odgovoran za:

9.3.1.1 ažuriranje ove politike i dokumentiranje svih izmjena uz vođenje povijesti verzija

9.3.1.2 obavještavanje osoblja, razvojnih inženjera i relevantnih pružatelja usluga o ažuriranjima

9.3.1.3 potvrdu da sve osobe uključene u aktivnosti povezane s testiranjem razumiju i primjenjuju najnovija pravila

9.3.1.4 održavanje dostupne verzije važeće politike za potrebe pregleda i revizije

9.4 Revizija i dokumentacija

9.4.1 Zapisi o svim pregledima politike, odobrenjima za uporabu stvarnih podataka i svim obrazloženjima iznimaka moraju biti:

9.4.1.1 sigurno pohranjeni za potrebe revizije

9.4.1.2 dostupni na zahtjev tijekom unutarnjih revizija ili revizija trećih strana

9.4.1.3 pregledani jednom godišnje radi osiguravanja dosljednosti s praksama testiranja

10. Povezane politike i poveznice

10.1 Ova politika mora se primjenjivati usklađeno sa sljedećim SME politikama radi održavanja sigurnosti i usklađenosti tijekom testiranja:

10.1.1 P2S – Politika uloga i odgovornosti u upravljanju: definira tko je odgovoran za nadzor razvoja, testiranja i odgovornosti za odvajanje sustava.

10.1.2 P4S – Politika kontrole pristupa: uređuje dodjelu, upravljanje i uklanjanje vjerodajnica za pristup testnim sustavima.

10.1.3 P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da osoblje razumije rizike povezane s testnim podacima, sigurne prakse postupanja i pravilno odvajanje okruženja.

10.1.4 P13S – Politika klasifikacije i označavanja podataka: podupire jasnu klasifikaciju testnih podataka i usmjerava strategije anonimizacije ili maskiranja podataka.

10.1.5 P17S – Politika zaštite podataka i privatnosti: usklađena je s obvezama prema GDPR-u, uključujući zaštitne mjere za obradu i pohranu osobnih podataka, uključujući i testna okruženja.

10.1.6 P24S – Politika sigurnog razvoja: utvrđuje opća sigurnosna očekivanja za razvojne timove, uključujući sigurno korištenje podataka tijekom faza testiranja.

10.1.7 P30S – Politika upravljanja incidentima: opisuje način odgovora na svaku povredu ili problem otkriven u testnom okruženju ili uzrokovan nepravilnim postupanjem s testnim podacima.

10.2 Ove politike čine jedinstven sigurnosni okvir za podršku cjelovitosti testiranja, minimizaciji podataka i potpunoj usklađenosti s ISO/IEC 27001 kroz razvojne i QA aktivnosti.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 6.1 – zahtijeva procjenu rizika i mjere obrade rizika, uključujući rizike povezane s testiranjem.

11.1.2 Točka 8.1 – zahtijeva planiranje i kontrolu operativnih procesa, uključujući okruženja za uspostavu testnih sustava.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.28 – zahtijeva da organizacije štite testne podatke i osiguraju da ne sadrže osjetljive podatke ili stvarne produkcijske podatke.

11.2.2 Kontrola 8.29 – zahtijeva jasno odvajanje razvojnih, testnih i produkcijskih okruženja.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – obuhvaća očekivanja u pogledu kontrola razvoja i testiranja.

11.3.2 SA-12 – odnosi se na rizike testiranja u opskrbnom lancu i sigurnosne evaluacije.

11.3.3 SC-32 – zahtijeva odvajanje okruženja i zaštitu povjerljivosti i cjelovitosti testnih podataka.

11.4 Opća uredba EU o zaštiti podataka (GDPR)

11.4.1 Članak 5(1)(c) – zahtijeva minimizaciju podataka, uključujući uporabu samo nužnih podataka za testiranje.

11.4.2 Članak 25 – zahtijeva zaštitu privatnosti u fazi projektiranja, što uključuje i kontrole testnih okruženja.

11.4.3 Članak 32 – zahtijeva sigurnu obradu osobnih podataka u svim sustavima, uključujući neprodukcijska okruženja.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(e), (h) – zahtijeva siguran razvoj i testiranje sustava, osobito kada su digitalne usluge izložene kibernetičkom riziku.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 9 – naglašava važnost digitalne operativne otpornosti, uključujući sigurno testiranje IKT sustava od strane SME subjekata u financijskom sektoru.

11.7 COBIT 2019

11.7.1 BAI07 – Upravljanje prihvaćanjem promjena i prijelazom: uključuje kontrole testiranja radi provjere novih sustava i postupanja s podacima.

11.7.2 DSS05 – Upravljanje sigurnosnim uslugama: zahtijeva testne i razvojne prakse koje sprječavaju zlouporabu ili izlaganje poslovnih podataka.