					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P29					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 propisima

Standard/propis	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Relevantno za sigurno planiranje i kontrolu testnih podataka i okruženja
ISO/IEC 27002:2022	Kontrole 8.28–8.29	Obuhvaća sigurnost testnih podataka i zaštitu testnih okruženja
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Obuhvaća testiranje i vrednovanje od strane razvojnih inženjera, zaštitu podataka u mirovanju i cjelovitost informacija
GDPR EU	Članci 5, 25, 32	Obuhvaća minimizaciju podataka, ugrađenu zaštitu privatnosti i sigurnost obrade u kontekstu testiranja
Direktiva EU NIS2	Članak 21(2)(e), (h)	Odnosi se na prakse sigurnog razvoja i testiranja
Uredba EU DORA	Članak 9	Odnosi se na IKT sustave i protokole te sigurnost testnih podataka
COBIT 2019	DSS05, BAI07	Obuhvaća upravljanje sigurnosnim uslugama te prihvaćanje i prijelaz promjena

1. Svrha

1.1. Ova politika utvrđuje obvezne zahtjeve za upravljanje testnim okruženjima i testnim podacima radi osiguravanja sigurnosti, povjerljivosti i operativne cjelovitosti tijekom cijelog životnog ciklusa razvoja softvera i testiranja.

1.2. Svrha ove politike jest spriječiti neovlašteni pristup, curenje podataka i kontaminaciju produkcijskih sustava uzrokovanu neprimjereno upravljanim testnim okruženjima ili uporabom stvarnih podataka u testiranju.

1.3. Ova politika propisuje sigurno postupanje s podacima koji se upotrebljavaju za testiranje, sigurno očvršćivanje testne infrastrukture i kontrolu pristupa temeljenu na ulogama (RBAC), uz usklađenost s primjenjivim regulatornim i ugovornim obvezama.

2. Područje primjene

2.1. Ova politika primjenjuje se na sva testna okruženja, podatke, alate i procese koji se upotrebljavaju za testiranje softvera, sustava, aplikacija i infrastrukture u cijeloj organizaciji.

2.2. Politika obuhvaća:

2.2.1. testna okruženja uspostavljena u vlastitoj infrastrukturi, u oblaku ili putem platformi trećih strana

2.2.2. testne podatke koji se upotrebljavaju u funkcionalnom testiranju, testiranju performansi, regresijskom testiranju i sigurnosnom testiranju

2.2.3. ručno, skriptirano ili automatizirano testiranje (npr. CI/CD cjevovodi)

2.2.4. sve osobe uključene u testiranje, uključujući interne timove, dobavljače i ugovorne izvođače

2.3. Ova politika primjenjuje se neovisno o kritičnosti sustava, vrsti aplikacije ili o tome provodi li se razvoj interno ili je ugovoren vanjski razvoj.

3. Ciljevi

3.1. Spriječiti uporabu stvarnih, osjetljivih ili reguliranih podataka (npr. PII, podaci o imateljima kartica) u testnim okruženjima, osim ako su anonimizirani ili posebno odobreni.

3.2. Osigurati potpunu mrežnu i pristupnu segmentaciju između testnih i produkcijskih okruženja kako bi se spriječio neovlašteni pristup podacima ili kontaminacija sustava.

3.3. Zahtijevati šifriranje, maskiranje podataka ili generiranje sintetičkih podataka kada su za potrebe testiranja nužni reprezentativni podaci.

3.4. Smanjiti vjerojatnost neusklađenosti, izloženosti podataka klijenata ili operativnih poremećaja koji proizlaze iz nesigurnih testnih podataka ili okruženja.

3.5. Uskladiti postupanje s testnim podacima s industrijskim standardima (ISO, NIST, COBIT) i propisima kao što su GDPR, NIS2 i DORA.

4. Uloge i odgovornosti

4.1. Glavni direktor za informacijsku sigurnost (CISO)

4.1.1. Vlasnik je ove politike i osigurava tehničke i administrativne zaštitne mjere za testne podatke i testna okruženja.

4.1.2. Odobrava uporabu stvarnih ili osjetljivih podataka u testiranju uz odgovarajuće obrazloženje i kompenzacijske kontrole.

4.2. Voditelji QA-a/testiranja

4.2.1. Koordiniraju planiranje testiranja i osiguravaju da su sve aktivnosti testiranja usklađene sa zahtjevima ove politike.

4.2.2. Provjeravaju odgovarajuću segmentaciju, pristup i pripremu podataka za svaku fazu testiranja.

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

9. Zahtjevi za pregled i ažuriranje

9.1. Ova politika mora se pregledavati najmanje jednom godišnje i ažurirati prema potrebi kako bi odražavala:

9.1.1. promjene regulatornih zahtjeva (npr. GDPR, DORA, NIS2)

9.1.2. uvođenje novih alata za testiranje, platformi ili automatizacijskih cjevovoda

9.1.3. nalaze interne revizije ili preporuke nakon incidenta

9.1.4. proširenje razvojnih ili QA procesa koje mijenja postupanje s testnim podacima ili uporabu okruženja

9.2. CISO je odgovoran za pokretanje pregleda u suradnji sa sljedećim ulogama:

9.2.1. voditelji QA-a/testiranja

9.2.2. DevOps i voditelji infrastrukture

9.2.3. timovi za razvoj aplikacija

9.2.4. službenik za zaštitu podataka (DPO) i pravni savjetnik

9.3. Sve izmjene moraju biti:

9.3.1. pod verzijskom kontrolom i pohranjene u središnjem repozitoriju dokumenata

9.3.2. priopćene relevantnom osoblju formalnim kanalima (npr. obavijesti ISMS-a, timski brifinzi)

9.3.3. povezane s ažuriranjima pripadajućih tehničkih standarda, kontrola i operativnih postupaka

9.4. Izvanredni pregledi pokrenuti događajem moraju se provesti odmah nakon bilo kojeg od sljedećih događaja:

9.4.1. curenja podataka ili povrede koja uključuje testna okruženja

9.4.2. nesukladnosti utvrđene revizijom povezane s postupanjem s testnim podacima

9.4.3. značajnih promjena u pravnim obvezama ili IT arhitekturi

10. Povezane politike i poveznice

10.1. Ova politika usko je povezana sa sljedećim politikama radi osiguravanja sigurnog i usklađenog postupanja s testnim podacima i testnim okruženjima:

10.1.1. P1 – Politika informacijske sigurnosti: utvrđuje nadređena sigurnosna načela koja uređuju zaštitu testnih podataka i upravljanje okruženjima.

10.1.2. P5 – Politika upravljanja promjenama: primjenjuje se na uspostavu, ažuriranje i stavljanje izvan uporabe testnih okruženja i cjevovoda za implementaciju.

10.1.3. P13 – Politika klasifikacije i označavanja podataka: usmjerava odabir testnih podataka i primjenu kontrola temeljenih na osjetljivosti.

10.1.4. P14 – Politika zadržavanja i zbrinjavanja podataka: određuje rokove zadržavanja i zahtjeve sigurnog zbrinjavanja za skupove testnih podataka.

10.1.5. P15 – Politika sigurnosnog kopiranja i vraćanja podataka: propisuje prakse sigurnosnog kopiranja i provjeru oporavka za testna okruženja.

10.1.6. P18 – Politika kriptografskih kontrola: utvrđuje obvezne standarde šifriranja za podatke u mirovanju i podatke u prijenosu unutar testnih platformi.

10.1.7. P22 – Politika zapisivanja događaja i praćenja: uređuje vidljivost i otkrivanje anomalija za aktivnosti u testnim okruženjima.

10.1.8. P30 – Politika odgovora na incidente: određuje eskalaciju i otklanjanje posljedica za povrede ili incidente koji uključuju testne sustave.

10.1.9. P33 – Politika praćenja revizije i usklađenosti: omogućuje provjeru usklađenosti s politikom i kontinuirano osiguranje djelotvornosti kontrola.

11. Referentni standardi i okviri

11.1. Ova politika usklađena je s globalnim standardima kibernetičke sigurnosti i regulatornim okvirima koji zahtijevaju sigurno postupanje s testnim podacima i zaštitu neprodukcijskih okruženja.

11.2. ISO/IEC 27001:

11.2.1. Točka 8.1 – Propisuje sigurno planiranje i kontrolu testnih podataka i okruženja.

11.3. ISO/IEC 27002:2022 – Kontrole 8.28–8.29:

11.3.1. Dodatak A, kontrola 8.28 – Sigurni testni podaci: zahtijeva zaštitu testnih podataka koji se upotrebljavaju u fazama razvoja i testiranja primjenom anonimizacije, maskiranja ili generiranja sintetičkih podataka.

11.3.2. Dodatak A, kontrola 8.29 – Zaštita testnih okruženja: zahtijeva odvajanje od produkcije, kontrolu pristupa i sigurno očvršćivanje okruženja za testne sustave.

11.3.3. Ove kontrole utvrđuju zahtjeve za sigurno upravljanje podacima koji se upotrebljavaju tijekom testiranja te za zaštitu neprodukcijskih sustava od zlouporabe, kompromitacije ili kontaminacije.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testiranje i vrednovanje od strane razvojnih inženjera: uspostavlja očekivanja za sigurne i ponovljive postupke testiranja uz odgovarajuće kontrole podataka.

11.4.2. SC-28 – Zaštita informacija u mirovanju: usklađeno je sa šifriranjem testnih podataka pohranjenih u neprodukcijskim sustavima.

11.4.3. SC-32 – Cjelovitost informacija: podupire provjeru podataka, sprječavanje oštećenja i ulazno-izlazne kontrole tijekom testiranja.

11.5. GDPR EU (2016/679):

11.5.1. Članak 5 – Minimizacija podataka: zabranjuje nepotrebnu uporabu osobnih podataka u testiranju.

11.5.2. Članak 25 – Ugrađena zaštita privatnosti: zahtijeva primjenu tehnika zaštite podataka od početka ciklusa razvoja i testiranja.

11.5.3. Članak 32 – Sigurnost obrade: propisuje zaštitne mjere za testna okruženja koja obrađuju osobne ili osjetljive podatke.

11.6. Direktiva EU NIS2 (2022/2555):

11.6.1. Članak 21(2)(e, h): zahtijeva sigurne procese razvoja softvera i testiranja, uz naglasak na zaštiti od neovlaštenog pristupa i curenja podataka.

11.7. Uredba EU DORA (2022/2554):

11.7.1. Članak 9 – IKT sustavi i protokoli: zahtijeva da procesi testiranja podupiru otpornost i štite operativne podatke od kompromitacije ili neovlaštenog otkrivanja.

11.8. COBIT 2019:

11.8.1. DSS05 – Upravljanje sigurnosnim uslugama: podupire provedbu sigurnosnih politika u svim okruženjima, uključujući neprodukcijska.

11.8.2. BAI07 – Upravljanje prihvaćanjem promjena i prijelazom: obuhvaća formalni postupak prijelaza iz testiranja u produkciju, uključujući kontrole podataka i okruženja.