					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P29					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	Klavzula 8	Povezano z varnim načrtovanjem in nadzorom testnih podatkov ter okolij
ISO/IEC 27002:2022	Kontrole 8.28–8.29	Obravnava varnost testnih podatkov in zaščito testnih okolij
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Obravnava testiranje in vrednotenje s strani razvijalcev, zaščito podatkov v mirovanju ter celovitost informacij
Uredba EU GDPR	Členi 5, 25, 32	Obravnava minimizacijo podatkov, varstvo zasebnosti že pri načrtovanju in varnost obdelave v kontekstu testiranja
Direktiva EU NIS2	Člen 21(2)(e), (h)	Povezano s praksami varnega razvoja in testiranja
Uredba EU DORA	Člen 9	Nanaša se na sisteme IKT, protokole in varnost testnih podatkov
COBIT 2019	DSS05, BAI07	Obravnava upravljanje varnostnih storitev ter prevzem in prehod sprememb

1. Namen

1.1. Ta politika določa obvezne zahteve za upravljanje testnih okolij in testnih podatkov, da se v celotnem življenjskem ciklu razvoja programske opreme in testiranja zagotovijo varnost, zaupnost in operativna celovitost.

1.2. Namen te politike je preprečiti nepooblaščen dostop, uhajanje podatkov in kontaminacijo produkcijskih sistemov zaradi neustrezno upravljanih testnih okolij ali uporabe dejanskih podatkov pri testiranju.

1.3. Ta politika zahteva varno ravnanje s podatki, ki se uporabljajo pri testiranju, varnostno utrjevanje testne infrastrukture in kontrole dostopa na podlagi vlog (RBAC), ob hkratnem zagotavljanju skladnosti z veljavnimi regulativnimi in pogodbenimi obveznostmi.

2. Področje uporabe

2.1. Ta politika se uporablja za vsa testna okolja, podatke, orodja in procese, ki se uporabljajo za testiranje programske opreme, sistemov, aplikacij in infrastrukture v celotni organizaciji.

2.2. Politika zajema:

2.2.1. testna okolja, vzpostavljena v lastni infrastrukturi, v oblaku ali prek platform tretjih oseb,

2.2.2. testne podatke, ki se uporabljajo pri funkcionalnem, zmogljivostnem, regresijskem in varnostnem testiranju,

2.2.3. ročno, skriptno ali avtomatizirano testiranje (npr. cevovodi CI/CD),

2.2.4. vse osebe, vključene v testiranje, vključno z internimi ekipami, dobavitelji in pogodbenimi izvajalci.

2.3. Ta politika se uporablja ne glede na kritičnost sistema, vrsto aplikacije ali to, ali se razvoj izvaja interno ali zunanje.

3. Cilji

3.1. Preprečiti uporabo produkcijskih, občutljivih ali reguliranih podatkov (npr. osebnih podatkov (PII), podatkov o imetnikih plačilnih kartic) v testnih okoljih, razen če so anonimizirani ali posebej odobreni.

3.2. Zagotoviti popolno omrežno in dostopovno ločitev med testnimi in produkcijskimi okolji, da se preprečita nepooblaščen dostop do podatkov ali kontaminacija sistemov.

3.3. Zahtevati šifriranje, maskiranje podatkov ali generiranje sintetičnih podatkov, kadar so za potrebe testiranja potrebni reprezentativni podatki.

3.4. Zmanjšati verjetnost neskladnosti, razkritja podatkov o strankah ali operativnih motenj zaradi neustreznih testnih podatkov ali okolij.

3.5. Uskladiti ravnanje s testnimi podatki s panožnimi standardi (ISO, NIST, COBIT) in predpisi, kot so GDPR, NIS2 in DORA.

4. Vloge in odgovornosti

4.1. vodja informacijske varnosti (CISO)

4.1.1. Je lastnik te politike in zagotavlja vzpostavitev tehničnih ter administrativnih zaščitnih ukrepov za testne podatke in okolja.

4.1.2. Odobrava uporabo dejanskih ali občutljivih podatkov pri testiranju ob ustrezni utemeljitvi in vzpostavljenih nadomestnih kontrolah.

4.2. vodje QA/testiranja

4.2.1. Usklajujejo načrtovanje testiranja in zagotavljajo, da so vse aktivnosti testiranja skladne z zahtevami te politike.

4.2.2. Preverjajo ustrezno ločitev, dostop in pripravo podatkov za vsako fazo testiranja.

[... 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. Ta politika mora biti pregledana letno in po potrebi posodobljena, da odraža:

9.1.1. spremembe regulativnih zahtev (npr. GDPR, DORA, NIS2),

9.1.2. uvedbo novih orodij, platform ali cevovodov za avtomatizacijo testiranja,

9.1.3. ugotovitve notranje presoje ali priporočila po incidentu,

9.1.4. širitev razvojnih ali QA-procesov, ki spreminjajo ravnanje s testnimi podatki ali uporabo okolij.

9.2. Vodja informacijske varnosti (CISO) je odgovoren za začetek pregleda v sodelovanju z:

9.2.1. vodji QA/testiranja,

9.2.2. vodji DevOps in infrastrukture,

9.2.3. ekipami za razvoj aplikacij,

9.2.4. pooblaščeno osebo za varstvo podatkov (DPO) in pravnim svetovalcem.

9.3. Vse revizije morajo biti:

9.3.1. upravljane z različicami in shranjene v osrednjem repozitoriju dokumentacije,

9.3.2. sporočene zadevnemu osebju po formalnih kanalih (npr. obvestila ISMS, obvestila ekipam),

9.3.3. povezane s posodobitvami povezanih tehničnih standardov, kontrol in operativnih postopkov.

9.4. Vmesni pregledi na podlagi sprožilcev morajo biti izvedeni takoj po katerem koli od naslednjih dogodkov:

9.4.1. uhajanju podatkov ali incidentu, povezanem s testnimi okolji,

9.4.2. ugotovljeni neskladnosti pri presoji, povezani z ravnanjem s testnimi podatki,

9.4.3. pomembnih spremembah pravnih obveznosti ali arhitekture IT.

10. Povezane politike in povezave

10.1. Ta politika je tesno povezana z naslednjimi politikami za zagotavljanje varnega in skladnega ravnanja s testnimi podatki in okolji:

10.1.1. P1 – P01 Politika informacijske varnosti: določa krovna načela informacijske varnosti, ki urejajo zaščito testnih podatkov in upravljanje okolij.

10.1.2. P5 – P05 Politika upravljanja sprememb: uporablja se za vzpostavitev, posodobitev in izločitev testnih okolij ter cevovodov uvajanja.

10.1.3. P13 – Politika klasifikacije in označevanja podatkov: usmerja izbiro testnih podatkov in uveljavljanje kontrol glede na občutljivost.

10.1.4. P14 – Politika hrambe podatkov in odstranjevanja: določa roke hrambe in zahteve za varno odstranjevanje testnih podatkovnih nizov.

10.1.5. P15 – Politika varnostnega kopiranja in obnove: določa zahteve glede varnostnega kopiranja in preverjanja obnovitve testnih okolij.

10.1.6. P18 – Politika kriptografskih kontrol: določa obvezne standarde šifriranja za podatke v mirovanju in med prenosom znotraj testnih platform.

10.1.7. P22 – Politika beleženja in spremljanja: ureja vidnost in zaznavanje anomalij pri aktivnostih v testnih okoljih.

10.1.8. P30 – Politika odzivanja na incidente: določa eskalacijo in odpravo pomanjkljivosti pri kršitvah ali incidentih, povezanih s testnimi sistemi.

10.1.9. P33 – Politika spremljanja presoj in skladnosti: omogoča preverjanje upoštevanja politike in stalno zagotavljanje ustreznosti.

11. Referenčni standardi in okviri

11.1. Ta politika je usklajena z globalnimi standardi kibernetske varnosti in regulativnimi okviri, ki zahtevajo varno ravnanje s testnimi podatki in zaščito neprodukcijskih okolij.

11.2. ISO/IEC 27001:

11.2.1. Klavzula 8.1 – zahteva varno načrtovanje in nadzor testnih podatkov ter okolij.

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

11.3.1. Priloga A, Kontrola 8.28 – Varni testni podatki: zahteva zaščito testnih podatkov, ki se uporabljajo v fazah razvoja in testiranja, z anonimizacijo, maskiranjem ali generiranjem sintetičnih podatkov.

11.3.2. Priloga A, Kontrola 8.29 – Zaščita testnih okolij: zahteva ločitev od produkcije, kontrole dostopa in utrjevanje okolij za testne sisteme.

11.3.3. Te kontrole določajo zahteve za varno upravljanje podatkov, ki se uporabljajo med testiranjem, ter za zaščito neprodukcijskih sistemov pred neprimerno uporabo, kompromitacijo ali kontaminacijo.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testiranje in vrednotenje s strani razvijalcev: določa pričakovanja glede varnih in ponovljivih postopkov testiranja z ustreznimi kontrolami nad podatki.

11.4.2. SC-28 – Zaščita informacij v mirovanju: usklajuje se s šifriranjem testnih podatkov, shranjenih v neprodukcijskih sistemih.

11.4.3. SC-32 – Celovitost informacij: podpira preverjanje podatkov, preprečevanje poškodb podatkov ter vhodno-izhodne kontrole med testiranjem.

11.5. Uredba EU GDPR (2016/679):

11.5.1. Člen 5 – minimizacija podatkov: prepoveduje nepotrebno uporabo osebnih podatkov pri testiranju.

11.5.2. Člen 25 – varstvo zasebnosti že pri načrtovanju: zahteva uporabo tehnik varstva podatkov od začetka razvojnega in testnega cikla.

11.5.3. Člen 32 – varnost obdelave: zahteva zaščitne ukrepe za testna okolja, ki obdelujejo osebne ali občutljive podatke.

11.6. Direktiva EU NIS2 (2022/2555):

11.6.1. Člen 21(2)(e, h): zahteva varne procese razvoja programske opreme in testiranja s poudarkom na zaščiti pred nepooblaščenim dostopom in uhajanjem podatkov.

11.7. Uredba EU DORA (2022/2554):

11.7.1. Člen 9 – sistemi IKT in protokoli: zahteva, da procesi testiranja podpirajo odpornost in varujejo operativne podatke pred kompromitacijo ali nepooblaščenim razkritjem.

11.8. COBIT 2019:

11.8.1. DSS05 – Upravljanje varnostnih storitev: podpira izvajanje varnostnih politik v vseh okoljih, vključno z neprodukcijskimi.

11.8.2. BAI07 – Upravljanje prevzema sprememb in prehoda: obravnava formalni proces prehoda iz testiranja v produkcijo, vključno s kontrolami podatkov in okolij.