					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P29S					Dokumendi pealkiri: **Testandmete ja testkeskkonna poliitika – VKE**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.1, 8	
ISO/IEC 27002:2022	Kontrollimeetmed 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
ELi GDPR	Artiklid 5(1)(c), 25, 32	
ELi NIS2	Artikli 21 lõike 2 punktid e ja h	
ELi DORA	Artikkel 9	
COBIT 2019	BAI07, DSS05	

1. Eesmärk

1.1 Käesolev poliitika määratleb, kuidas testandmeid ja testkeskkondi tuleb hallata, et vältida testimistegevuse käigus andmete juhuslikku avalikustamist, andmekaitserikkumisi või tegevushäireid.

1.2 See tagab, et tarkvara või süsteemide testimisel ei kasutata tegelikke kliendiandmeid sobimatul viisil ning et testkeskkonnad on tootmiskeskkondadest loogiliselt ja tehniliselt eraldatud.

1.3 Poliitika eesmärk on aidata VKE-del täita ISO/IEC 27001 sertifitseerimise nõudeid ja asjakohaseid andmekaitsealaseid õigusakte, jäädes samal ajal praktiliseks ja rakendatavaks organisatsioonides, kus puudub eraldiseisev IT-meeskond.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmise suhtes:

2.1.1 kõik testkeskkonnad (nt vahekeskkonna serverid, liivakastkeskkonnad, arenduse testkeskkonnad);

2.1.2 kõik testandmed, sõltumata sellest, kas need on loodud käsitsi, genereeritud või tuletatud aktiivkasutuses olevatest andmetest;

2.1.3 kogu testimistegevuses osalev personal, sealhulgas töötajad, töövõtjad, vabakutselised ja IT-teenuse osutajad;

2.1.4 igasugune testimine, mis võib mõjutada kliendile suunatud platvorme, sisemisi ärisüsteeme või kolmandate osapoolte teenuseid.

2.2 See hõlmab nii tehnilisi keskkondi kui ka protsesse, mida kasutatakse järgmise toetamiseks:

2.2.1 veebilehtede, rakenduste ja tööriistade arendus;

2.2.2 süsteemiuuendused, konfiguratsiooni testimine ja integratsioonitestimine;

2.2.3 automatiseeritud ja käsitsi teostatavad funktsionaalsed testid või turbetestid.

3. Eesmärgid

3.1 Vältida tegelike, tuvastatavate kliendiandmete kasutamist testimisel, välja arvatud juhul, kui andmed on anonüümitud ja selleks on antud selgesõnaline heakskiit.

3.2 Säilitada range eraldatus test- ja tootmissüsteemide vahel, et vältida soovimatut andmete avalikustamist või häireid tööprotsessides.

3.3 Kaitsta testsüsteeme ja testandmeid loata juurdepääsu, juhusliku avalikustamise või keskkondade vahelise korduskasutuse eest ilma asjakohaste kontrollimeetmeteta.

3.4 Täita kohaldatavaid andmekaitsenõudeid (nt GDPR, NIS2), tagades, et kõiki testandmeid töödeldakse õiguspäraselt, õiglaselt ja turvaliselt.

3.5 Toetada organisatsiooni auditivalmidust välisauditite ja ISO/IEC 27001 sertifitseerimise jaoks, dokumenteerides testimistavad ja rakendades järjepidevaid kaitsemeetmeid.

4. Rollid ja vastutused

4.1 tegevjuht

4.1.1 Vastutab üldiselt testandmete kaitse ja testsüsteemide turvalisuse eest.

4.1.2 Kiidab heaks tegelike andmete kasutamise testimisel pärast asjakohaste kaitsemeetmete olemasolu kinnitamist (nt anonüümimine või andmete maskeerimine).

4.1.3 Kontrollib, et testimistegevused on nõuetekohaselt dokumenteeritud ja vastavad käesolevale poliitikale.

4.2 projektiomanik

4.2.1 Koordineerib testimisprotsesside kavandamist ja elluviimist.

4.2.2 Tagab, et kõik meeskonnaliikmed mõistavad ja järgivad käesolevat poliitikat.

4.2.3 Kinnitab enne testimise algust, et testsüsteemid on turvaliselt seadistatud.

4.2.4 Teatab tegevjuhile kõigist testkeskkondade või andmeleketega seotud intsidentidest.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Planeeritud läbivaatamised

9.1.1 Käesolev poliitika tuleb tegevjuhi poolt läbi vaadata vähemalt üks kord aastas. Läbivaatamise eesmärk on tagada, et poliitika püsib ajakohane järgmise suhtes:

9.1.1.1 muudatused tarkvaraarenduse tööriistades, platvormides või keskkondades;

9.1.1.2 ajakohastatud õiguslikud kohustused, sealhulgas andmekaitse- või digitaalse toimepidevuse nõuded;

9.1.1.3 VKE sertifitseerimine ja auditivalmidus vastavalt ISO/IEC 27001-le.

9.2 Vahepealse läbivaatamise alused

9.2.1 Täiendavad läbivaatamised tuleb teha pärast järgmist:

9.2.1.1 mis tahes intsidenti, mis hõlmab andmete avalikustamist või kompromiteerimist testkeskkondades;

9.2.1.2 tegelike andmete kasutamist testimisel, isegi kui andmed on anonüümitud;

9.2.1.3 uute testimismeetodite, süsteemide või tarnijate kasutuselevõttu;

9.2.1.4 regulatiivseid muudatusi, mis mõjutavad andmete käitlemist testimise ajal.

9.3 Muudatuste juhtimine ja teabevahetus

9.3.1 Tegevjuht vastutab järgmise eest:

9.3.1.1 käesoleva poliitika ajakohastamine ja kõigi muudatuste dokumenteerimine versiooniajaloos;

9.3.1.2 töötajate, arendajate ja asjakohaste teenuseosutajate teavitamine muudatustest;

9.3.1.3 kinnitamine, et kõik testimisega seotud töötajad mõistavad ja rakendavad uusimaid nõudeid;

9.3.1.4 poliitika uusima versiooni kättesaadavana hoidmine läbivaatamise ja auditi eesmärgil.

9.4 Audit ja dokumentatsioon

9.4.1 Kõigi poliitika läbivaatamiste, tegelike andmete kasutamise heakskiitude ja erandite põhjenduste kirjed peavad olema:

9.4.1.1 turvaliselt säilitatud auditi eesmärgil;

9.4.1.2 taotluse korral kättesaadavad sise- või kolmanda osapoole auditite käigus;

9.4.1.3 igal aastal läbi vaadatud, et tagada kooskõla testimistavadega.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat tuleb testimise ajal turvalisuse ja vastavuse tagamiseks rakendada kooskõlas järgmiste VKE poliitikatega:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb, kes vastutab arenduse, testimise ja süsteemide eraldamise kohustuste järelevalve eest.

10.1.2 P4S – Juurdepääsukontrolli poliitika: reguleerib testsüsteemide autentimisandmete määramist, haldamist ja eemaldamist.

10.1.3 P8S – Infoturbeteadlikkuse ja koolituse poliitika: tagab, et töötajad mõistavad testandmetega seotud riske, turvalise käitlemise tavasid ja keskkondade nõuetekohast eraldamist.

10.1.4 P13S – Andmete klassifitseerimise ja märgistamise poliitika: toetab testandmete selget klassifitseerimist ning suunab anonüümimise või andmete maskeerimise strateegiaid.

10.1.5 P17S – Andmekaitse ja privaatsuse poliitika: tagab kooskõla GDPRi kohustustega, sealhulgas isikuandmete töötlemise ja säilitamise kaitsemeetmed ka testkeskkondades.

10.1.6 P24S – Turvalise arenduse poliitika: sätestab üldised turbenõuded arendusmeeskondadele, sealhulgas andmete turvalise kasutamise testimisfaasides.

10.1.7 P30S – Intsidentidele reageerimise poliitika: kirjeldab, kuidas reageerida testkeskkonnas avastatud rikkumisele või probleemile või vale testandmete käitlemise tõttu tekkinud juhtumile.

10.2 Need poliitikad moodustavad ühtse turberaamistiku, mis toetab testimise terviklust, andmete minimaalsust ja täielikku kooskõla ISO/IEC 27001 nõuetega arendus- ja kvaliteeditagamise tegevustes.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1 – nõuab riskihindamist ja riskikäsitluse tegevusi, sealhulgas testimisega seotud riskide käsitlemist.

11.1.2 Punkt 8.1 – nõuab tegevusprotsesside, sealhulgas testsüsteemide kasutuselevõtu keskkondade planeerimist ja kontrolli.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeede 8.28 – nõuab, et organisatsioonid kaitseksid testandmeid ja tagaksid, et need ei sisalda tundlikke andmeid ega aktiivkasutuses olevaid tootmisandmeid.

11.2.2 Kontrollimeede 8.29 – nõuab arendus-, test- ja tootmiskeskkondade selget eraldamist.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – hõlmab arenduse ja testimise kontrollinõudeid.

11.3.2 SA-12 – käsitleb tarneahela testimise riske ja turvahindamisi.

11.3.3 SC-32 – nõuab keskkondade eraldamist ning testandmete konfidentsiaalsuse ja tervikluse kaitset.

11.4 Euroopa Liidu isikuandmete kaitse üldmäärus (GDPR)

11.4.1 Artikkel 5(1)(c) – nõuab andmete minimaalsust, sealhulgas testimiseks ainult vajalike andmete kasutamist.

11.4.2 Artikkel 25 – nõuab lõimitud andmekaitset, mis hõlmab ka testkeskkondade kontrollimeetmeid.

11.4.3 Artikkel 32 – nõuab isikuandmete turvalist töötlemist kõigis süsteemides, sealhulgas tootmisvälistes keskkondades.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21 lõike 2 punktid e ja h – nõuab turvalist arendust ja süsteemide testimist, eriti juhtudel, kus digiteenused on avatud küberriskidele.

11.6 ELi DORA määrus (2022/2554)

11.6.1 Artikkel 9 – rõhutab digitaalse tegevustalitluse toimepidevuse olulisust, sealhulgas IKT-süsteemide turvalist testimist finantssektori VKE-des.

11.7 COBIT 2019

11.7.1 BAI07 – muudatuste vastuvõtmise ja ülemineku haldamine: hõlmab testimise kontrollimeetmeid uute süsteemide ja andmekäitluse valideerimiseks.

11.7.2 DSS05 – turvateenuste haldamine: nõuab testimis- ja arendustavasid, mis väldivad äriandmete väärkasutust või avalikustamist.