					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P29					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 õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Asjakohane testandmete ja testkeskkondade turvalise kavandamise ning kontrolli seisukohalt
ISO/IEC 27002:2022	Kontrollimeetmed 8.28–8.29	Käsitleb testandmete turvalist kasutamist ja testkeskkondade kaitset
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Käsitleb arendaja testimist ja hindamist, andmete kaitset puhkeolekus ning terviklust
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5, 25, 32	Käsitleb andmete minimaalsust, lõimitud andmekaitset ja töötlemise turvalisust testimise kontekstis
ELi NIS2 direktiiv	Artikkel 21(2)(e), (h)	Seotud turvalise arenduse ja testimise praktikatega
ELi DORA määrus	Artikkel 9	Käsitleb IKT-süsteeme, protokolle ja testandmete turvet
COBIT 2019	DSS05, BAI07	Käsitleb turvateenuste haldamist ning muudatuste vastuvõtmist ja üleminekut

1. Eesmärk

1.1. Käesolev poliitika sätestab kohustuslikud nõuded testkeskkondade ja testandmete haldamiseks, et tagada turvalisus, konfidentsiaalsus ja tegevuse terviklus kogu tarkvaraarenduse ja testimise elutsükli vältel.

1.2. Poliitika eesmärk on vältida loata juurdepääsu, andmeleket ning tootmissüsteemide saastumist puudulikult hallatud testkeskkondade või tegelike andmete kasutamise tõttu testimisel.

1.3. Poliitika nõuab testimisel kasutatavate andmete turvalist käitlemist, testtaristu kõvendamist ja rollipõhise juurdepääsukontrolli rakendamist ning on kooskõlas kohalduvate regulatiivsete ja lepinguliste kohustustega.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigi testkeskkondade, andmete, tööriistade ja protsesside suhtes, mida organisatsioonis kasutatakse tarkvara, süsteemide, rakenduste ja taristu testimiseks.

2.2. Poliitika hõlmab:

2.2.1. testkeskkondi, mis on juurutatud kohapealses taristus, pilvekeskkonnas või kolmandate osapoolte platvormidel;

2.2.2. testandmeid, mida kasutatakse funktsionaalsus-, jõudlus-, regressiooni- ja turbetestimisel;

2.2.3. käsitsi tehtavat, skriptipõhist või automatiseeritud testimist (nt CI/CD torustikud);

2.2.4. kogu testimisse kaasatud personali, sealhulgas sisemisi meeskondi, tarnijaid ja töövõtjaid.

2.3. Poliitika kehtib sõltumata süsteemi kriitilisusest, rakenduse tüübist või sellest, kas arendus toimub organisatsioonisiseselt või allhanke korras.

3. Eesmärgid

3.1. Vältida aktiivkasutuses olevate, tundlike või reguleeritud andmete (nt isikut tuvastav teave, kaardiomaniku andmed) kasutamist testkeskkondades, välja arvatud juhul, kui andmed on anonüümseks muudetud või selleks on antud eraldi heakskiit.

3.2. Tagada test- ja tootmiskeskkondade täielik võrgu- ja juurdepääsuõiguste eraldatus, et vältida loata juurdepääsu andmetele või süsteemide saastumist.

3.3. Nõuda krüptimise, andmete maskeerimise või sünteetiliste andmete genereerimise kasutamist, kui testimiseks on vaja representatiivseid andmeid.

3.4. Vähendada nõuetele vastavuse rikkumiste, kliendiandmete avalikuks saamise või tegevushäirete tõenäosust, mis tuleneb ebaturvalistest testandmetest või testkeskkondadest.

3.5. Viia testandmete käitlemine kooskõlla valdkonna standardite (ISO, NIST, COBIT) ning regulatsioonidega, nagu GDPR, NIS2 ja DORA.

4. Rollid ja vastutused

4.1. Infoturbejuht

4.1.1. Vastutab käesoleva poliitika eest ning rakendab testandmete ja testkeskkondade jaoks tehnilised ja korralduslikud meetmed.

4.1.2. Kiidab asjakohase põhjenduse ja kompenseerivate kontrollimeetmete olemasolul heaks tegelike või tundlike andmete kasutamise testimisel.

4.2. QA- ja testimisjuhid

4.2.1. Koordineerivad testimise kavandamist ja tagavad, et kõik testimistegevused vastavad käesoleva poliitika nõuetele.

4.2.2. Valideerivad iga testimisetapi jaoks nõuetekohase eraldatuse, juurdepääsuõigused ja andmete ettevalmistuse.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata ja vajaduse korral ajakohastada, et arvesse võtta:

9.1.1. muudatusi regulatiivsetes nõuetes (nt GDPR, DORA, NIS2);

9.1.2. uute testimistööriistade, platvormide või automatiseerimistorustike kasutuselevõttu;

9.1.3. siseauditi leide või intsidendijärgseid soovitusi;

9.1.4. arendus- või QA-protsesside laiendamist, mis muudab testandmete käitlemist või keskkondade kasutamist.

9.2. Läbivaatamise algatamise eest vastutab infoturbejuht koostöös järgmiste osapooltega:

9.2.1. QA- ja testimisjuhid;

9.2.2. DevOpsi ja taristu juhid;

9.2.3. rakenduste arendusmeeskonnad;

9.2.4. andmekaitseametnik ja õigusnõustaja.

9.3. Kõik muudatused peavad olema:

9.3.1. versioonihalduse all ja salvestatud kesksesse dokumendihoidlasse;

9.3.2. edastatud mõjutatud personalile ametlike kanalite kaudu (nt ISMS-i teavitused, meeskonna briifingud);

9.3.3. seotud vastavate tehniliste standardite, kontrollimeetmete ja tööprotseduuride ajakohastustega.

9.4. Sündmuspõhised vahepealsed läbivaatused tuleb teha viivitamata pärast:

9.4.1. andmeleket või rikkumist, mis hõlmab testkeskkondi;

9.4.2. testandmete käitlemisega seotud auditi mittevastavust;

9.4.3. olulisi muudatusi õiguslikes kohustustes või IT-arhitektuuris.

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika on tihedalt seotud järgmiste poliitikatega, et tagada testandmete ja testkeskkondade turvaline ning nõuetele vastav käitlemine:

10.1.1. P1 – infoturbepoliitika: kehtestab üldised turbepõhimõtted, mis reguleerivad testandmete kaitset ja keskkondade haldamist.

10.1.2. P5 – muudatuste haldamise poliitika: kehtib testkeskkondade loomise, ajakohastamise, kasutuselt kõrvaldamise ja juurutustorustike suhtes.

10.1.3. P13 – andmete klassifitseerimise ja märgistamise poliitika: suunab testandmete valikut ja tundlikkusel põhinevate kontrollimeetmete rakendamist.

10.1.4. P14 – andmete säilitamise ja kõrvaldamise poliitika: määrab testandmestike säilitustähtajad ja turvalise kõrvaldamise nõuded.

10.1.5. P15 – varundamise ja taastamise poliitika: nõuab testkeskkondade varundamistavasid ja taaste valideerimist.

10.1.6. P18 – krüptograafiliste kontrollimeetmete poliitika: määrab kindlaks kohustuslikud krüptimisstandardid andmetele puhkeolekus ja edastamisel testplatvormidel.

10.1.7. P22 – logimise ja seire poliitika: reguleerib testkeskkondade tegevuste nähtavust ja anomaaliate tuvastamist.

10.1.8. P30 – intsidentidele reageerimise poliitika: määratleb rikkumiste või testisüsteeme hõlmavate intsidentide eskaleerimise ja puuduste kõrvaldamise.

10.1.9. P33 – auditi ja nõuetele vastavuse seire poliitika: võimaldab valideerida poliitika järgimist ja tagada pidev vastavus.

11. Viitestandardid ja raamistikud

11.1. Käesolev poliitika on kooskõlas üleilmsete küberturbe standardite ja regulatiivsete raamistikega, mis nõuavad testandmete turvalist käitlemist ja tootmisväliste keskkondade kaitset.

11.2. ISO/IEC 27001:

11.2.1. Punkt 8.1 – nõuab testandmete ja testkeskkondade turvalist kavandamist ja kontrolli.

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

11.3.1. Lisa A kontrollimeede 8.28 – turvalised testandmed: nõuab arendus- ja testimisetappides kasutatavate testandmete kaitset anonüümimise, maskeerimise või sünteetilise genereerimise kaudu.

11.3.2. Lisa A kontrollimeede 8.29 – testkeskkondade kaitse: nõuab testsüsteemide eraldamist tootmiskeskkonnast, juurdepääsukontrolli ja keskkonna kõvendamist.

11.3.3. Need kontrollimeetmed kirjeldavad nõudeid testimisel kasutatavate andmete turvaliseks haldamiseks ja tootmisväliste süsteemide kaitsmiseks väärkasutuse, kompromiteerimise või saastumise eest.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – arendaja testimine ja hindamine: kehtestab ootused turvalistele, korratavatele testimisprotsessidele koos asjakohaste andmekontrollidega.

11.4.2. SC-28 – teabe kaitse puhkeolekus: on kooskõlas tootmisvälistes süsteemides salvestatud testandmete krüptimisega.

11.4.3. SC-32 – teabe terviklus: toetab andmete valideerimist, riknemise vältimist ning sisendi- ja väljundikontrolle testimise käigus.

11.5. ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679):

11.5.1. Artikkel 5 – andmete minimaalsus: keelab isikuandmete ebavajaliku kasutamise testimisel.

11.5.2. Artikkel 25 – lõimitud andmekaitse: nõuab andmekaitsemeetodite rakendamist alates arendus- ja testimistsükli algusest.

11.5.3. Artikkel 32 – töötlemise turvalisus: nõuab kaitsemeetmeid testkeskkondadele, kus käideldakse isikuandmeid või tundlikke andmeid.

11.6. ELi NIS2 direktiiv (2022/2555):

11.6.1. Artikkel 21(2)(e, h): nõuab turvalisi tarkvaraarenduse ja testimise protsesse, rõhutades kaitset loata juurdepääsu ja andmelekkete eest.

11.7. ELi DORA määrus (2022/2554):

11.7.1. Artikkel 9 – IKT-süsteemid ja protokollid: nõuab, et testimisprotsessid toetaksid toimepidevust ja kaitseksid tegevusandmeid kompromiteerimise või loata avalikustamise eest.

11.8. COBIT 2019:

11.8.1. DSS05 – turvateenuste haldamine: toetab turbepoliitikate rakendamist kõigis keskkondades, sealhulgas tootmisvälistes keskkondades.

11.8.2. BAI07 – muudatuste vastuvõtmise ja ülemineku haldamine: käsitleb ametlikku üleminekut testimisest tootmiskeskkonda, sealhulgas andmete ja keskkondade kontrollimeetmeid.