					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P16					Dokumendi pealkiri: **Andmete maskeerimise ja pseudonüümimise poliitika**						
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/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 6.1	Üldnõuded riskijuhtimisele ja operatiivsetele kontrollimeetmetele maskeerimise ja pseudonüümimise rakendamisel
ISO/IEC 27002:2022	Kontrollimeetmed 8.11, 8	Kontrollimeetmete juhised maskeerimise ja pseudonüümimise rakendamiseks
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Andmekaitse ja konfidentsiaalsuse kontrollimeetmed andmete minimeerimiseks, teisendamiseks ja juurdepääsu piiramiseks
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 4(5), 5(1)(c,f), 32	Pseudonüümimise ja andmekaitsemeetmete õiguslik alus ning nõuded
ELi NIS2 direktiiv	Artikkel 21(2)(c)	Kohustus rakendada tehnilisi ja korralduslikke meetmeid, sealhulgas privaatsust suurendavaid tehnoloogiaid (PET-id)
ELi DORA määrus	Artiklid 10(1), 10(2)(e)	IKT-riskide juhtimine ja konfidentsiaalsuse kontrollimeetmed andmete maskeerimiseks ning pseudonüümimiseks
COBIT 2019	DSS05.01, DSS06.06, MEA	Juhtimiskontrollid andmekaitseks maskeerimise abil ja vastavuse hindamiseks

1. Eesmärk

1.1 Käesolev poliitika määratleb organisatsiooni lähenemise andmete maskeerimise ja pseudonüümimise rakendamisele privaatsust suurendavate tehnoloogiatena (PET-id), et vähendada isikute tuvastatavust ning isikuandmete või muu tundliku teabe kokkupuudet.

1.2 Poliitika toetab teabe turvalist kasutamist testimises, analüütikas ja tegevusprotsessides, tagades samal ajal vastavuse õiguslikele ja regulatiivsetele nõuetele, vähendades rikkumiste mõju ning rakendades andmete minimeerimise ja konfidentsiaalsuse põhimõtteid.

1.3 Poliitika on kooskõlas standardiga ISO/IEC 27001:2022, toetab GDPR-i artiklit 4(5) pseudonüümimise kohta ning lõimib riskipõhise rakendamise kooskõlas NIST-i, NIS2, DORA ja COBIT 2019 raamistikuga.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmistele osapooltele ja valdkondadele:

2.1.1 kõigile töötajatele, töövõtjatele, kolmandatele isikutele ja tarnijatele, kellel on juurdepääs süsteemidele, mis töötlevad isikuandmeid, konfidentsiaalset või tundlikku teavet;

2.1.2 kõigile andmekeskkondadele, sealhulgas tootmis-, arendus-, testimis- ja vahekeskkondadele;

2.1.3 kõigile andmete maskeerimise vormidele (nt staatiline, dünaamiline, deterministlik, tokeniseerimine) ning pseudonüümimise meetoditele, mida kasutatakse andmekaitseriskide vähendamiseks;

2.1.4 kõigile andmeliikidele (struktureeritud või struktureerimata), süsteemidele (kohapealsetele või pilvekeskkonnas majutatutele) ja rakendustele, mis hõlmavad isikuandmeid või reguleeritud andmeid.

2.2 Kohaldamisala hõlmab kasutust järgmistes valdkondades:

2.2.1 rakenduste arenduse ning QA/testimise keskkondades;

2.2.2 analüütika- või aruandlusplatvormidel;

2.2.3 andmevahetuses kolmandate isikute või teenuseosutajatega;

2.2.4 varundus-, arhiveerimis- või taastesüsteemides.

3. Eesmärgid

3.1 Tagada maskeerimise ja pseudonüümimise järjepidev ja tõhus rakendamine, et vähendada andmete kokkupuute või väärkasutuse riski.

3.2 Tagada, et tootmisvälistes keskkondades ei kasutata kunagi tegelikke andmeid, välja arvatud juhul, kui need on teisendatud heakskiidetud PET-meetodite abil.

3.3 Säilitada viiteterviklus, kasutatavus ja vormingut säilitavad teisendused, kui see on vajalik tegevuse järjepidevuse tagamiseks.

3.4 Rakendada ranget juurdepääsukontrolli algandmetele, maskeeritud andmetele ja taasidentifitseerimise võtmetele.

3.5 Käsitleda maskeeritud või pseudonüümitud andmestikke tundlike andmetena, mille suhtes kohaldatakse juurdepääsulogisid, säilitamiskontrolle ja intsidendihalduse protseduure.

3.6 Valideerida nende kontrollimeetmete tõhusus pideva testimise, seire ja auditiprotseduuride kaudu.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 kiidab käesoleva poliitika heaks ja tagab selle rakendamise osana laiemast IT juhtimisest ja andmekaitse algatustest.

4.2 infoturbejuht / ISMS-i juht

4.2.1 teostab järelevalvet rakendamise ja pideva vastavuse üle;

4.2.2 tagab kooskõla standardi ISO/IEC 27001 punktiga 6.1.3 (riskikäsitlus) ja punktiga 8.1 (operatiivjuhtimine);

4.2.3 vaatab läbi auditilogid ja valideerib kontrollimeetmete tõhususe.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt üks kord aastas või varem, kui toimub mõni järgmistest sündmustest:

9.1.1 regulatiivsed muudatused, mis mõjutavad maskeerimist või pseudonüümimist;

9.1.2 tundlikke andmeid töötlevate uute IT-süsteemide kasutuselevõtt;

9.1.3 organisatsiooni andmete klassifitseerimisskeemi olulised muudatused;

9.1.4 auditileiud, mis viitavad kontrollimeetmete puudustele;

9.1.5 uute ohtude või maskeerimistehnoloogiate esilekerkimine.

9.2 ISMS-i juht juhib läbivaatamist koostöös andmekaitseametniku, andmeomanike, IT-turbe ning õigus- ja vastavusfunktsiooniga. Muudatused peavad olema versioonihalduses, tippjuhtkonna poolt heaks kiidetud ja kõigile asjakohastele sidusrühmadele teatavaks tehtud.

10. Seotud poliitikad ja seosed

10.1 P13 - Andmete klassifitseerimise ja märgistamise poliitika. Maskeerimise ja pseudonüümimise otsused sõltuvad otseselt P13-s määratletud andmeväljade klassifikatsioonist ja tundlikkustasemetest.

10.2 P14 - Andmete säilitamise ja kõrvaldamise poliitika. Teisendatud andmestikke tuleb säilitada ja kõrvaldada kooskõlas P14 elutsükli reeglitega, tagades, et maskeeritud ja pseudonüümitud andmeid käsitletakse tundlike andmetena.

10.3 P17 - Andmekaitse ja privaatsuse poliitika. Määratleb andmekaitse põhimõtted ja regulatiivse aluse pseudonüümimise rakendamiseks GDPR-i ja sarnaste õigusnormide kohase andmetöötlustoiminguna.

10.4 P22 - Logimise ja seire poliitika. Võimaldab tsentraliseeritud auditeerimist ja teavitamist maskeerimise ning pseudonüümimise sündmustest kooskõlas struktureeritud turvaseire protseduuridega.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 6.1.3 - riskikäsitluse plaan: määratleb maskeerimise ja pseudonüümimise riskikäsitluse meetmetena, et vähendada tundlike andmete tuvastatavust mitteolulistes töötlemiskeskkondades.

11.1.2 Punkt 8.1 - operatiivne planeerimine ja juhtimine: nõuab tehnilisi ja protseduurilisi kontrollimeetmeid andmete turvaliseks teisendamiseks töötlemise, salvestamise või edastamise käigus.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollimeetmed 8.11, 8: juhised andmete maskeerimiseks ja pseudonüümimiseks, et minimeerida taasidentifitseerimise ja andmelekkega seotud riske.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - isikut tuvastava teabe kaitse: privaatsust suurendavate tehnoloogiate, näiteks maskeerimise ja pseudonüümimise rakendamine.

11.3.2 PT-2, PT-3 - isikut tuvastava teabe töötlemise minimeerimine ja turvalisus: teisendamine tuvastatavuse vähendamiseks ja juurdepääsukontrolli rakendamiseks.

11.3.3 SC-12, SC-28, SC-30 - andmete konfidentsiaalsus ja terviklus: salvestamise, edastamise ja kasutamise konfidentsiaalsuse ning hägustamise kontrollimeetmed.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.4.1 Artikkel 4(5): pseudonüümimise ametlik määratlus.

11.4.2 Artikkel 32: töötlemise turvalisus - korralduslikud ja tehnilised meetmed pseudonüümimiseks.

11.4.3 Artikkel 5(1)(c,f): andmete minimeerimine ja konfidentsiaalsus pseudonüümimise või maskeerimise abil.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(c): nõuab turvameetmetena PET-ide, näiteks maskeerimise ja pseudonüümimise kasutamist.

11.6 ELi DORA määrus (2022/2554)

11.6.1 Artikkel 10(1): IKT-riskijuhtimise raamistik hõlmab maskeerimise ja pseudonüümimise kontrollimeetmeid.

11.6.2 Artikkel 10(2)(e): nõuab teisendustehnoloogiate kasutamist isiku- ja finantsandmete kaitseks.

11.7 COBIT 2019

11.7.1 DSS05.01: teabevarade kaitse - nõuded maskeerimisele ja pseudonüümimisele.
11.7.2 DSS06.06: turvaline testimine ja analüütika - maskeerimine tootmisvälistes keskkondades.
11.7.3 MEA03: vastavuse seire maskeerimise ja pseudonüümimise tõhususe hindamiseks.