					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P16					Název dokumentu: **Politika maskování dat a pseudonymizace**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Článek 6.1	Obecné požadavky na řízení rizik a provozní opatření pro maskování a pseudonymizaci
ISO/IEC 27002:2022	Opatření 8.11, 8	Pokyny k zavedení maskování a pseudonymizace
NIST SP 800-53 Rev. 5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Opatření k ochraně soukromí a důvěrnosti pro minimalizaci údajů, transformaci a omezení přístupu
GDPR	Články 4 odst. 5, 5 odst. 1 písm. c) a f), 32	Právní základ a požadavky na pseudonymizaci a opatření k ochraně údajů
směrnice NIS2	Článek 21 odst. 2 písm. c)	Povinnost zavést technická a organizační opatření, včetně technologií zvyšujících ochranu soukromí (PET)
nařízení DORA	Články 10 odst. 1, 10 odst. 2 písm. e)	Řízení rizik v oblasti ICT a opatření k zajištění důvěrnosti při maskování dat a pseudonymizaci
COBIT 2019	DSS05.01, DSS06.06, MEA	Opatření správy a řízení ochrany dat prostřednictvím maskování a posuzování souladu

1. Účel

1.1 Tato politika stanoví přístup organizace k zavádění maskování dat a pseudonymizace jako technologií zvyšujících ochranu soukromí (PET) za účelem snížení identifikovatelnosti a expozice osobních nebo citlivých údajů.

1.2 Podporuje bezpečné využívání informací při testování, analytice a provozu a současně zajišťuje soulad s právními a regulačními požadavky, zmírnění dopadů narušení bezpečnosti a uplatňování zásad minimalizace údajů a důvěrnosti.

1.3 Tato politika je v souladu s ISO/IEC 27001:2022, podporuje článek 4 odst. 5 GDPR týkající se pseudonymizace a zahrnuje implementaci založenou na rizicích v souladu s normami NIST, NIS2, DORA a COBIT 2019.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny zaměstnance, smluvní pracovníky, třetí strany a dodavatele s přístupem k systémům, které zpracovávají osobní, důvěrné nebo citlivé informace.

2.1.2 všechna datová prostředí, včetně produkčního, vývojového, testovacího a předprodukčního prostředí.

2.1.3 všechny formy maskování dat (např. statické, dynamické, deterministické, tokenizace) a techniky pseudonymizace používané ke snižování rizik pro soukromí.

2.1.4 všechny typy dat (strukturovaná i nestrukturovaná), systémy (on-premise nebo cloudové) a aplikace zahrnující osobní nebo regulovaná data.

2.2 Rozsah zahrnuje použití v:

2.2.1 vývoji aplikací a prostředích QA/testování,

2.2.2 analytických nebo reportingových platformách,

2.2.3 výměně dat s třetími stranami nebo poskytovateli služeb,

2.2.4 zálohovacích, archivačních nebo obnovovacích systémech.

3. Cíle

3.1 Zajistit konzistentní a účinné uplatňování maskování a pseudonymizace za účelem snížení rizika expozice dat nebo jejich zneužití.

3.2 Zajistit, aby skutečná data nebyla nikdy používána v neprodukčním prostředí, pokud nebyla transformována schválenými technikami PET.

3.3 Zachovat referenční integritu, použitelnost a transformace se zachováním formátu, pokud je to vyžadováno z důvodu provozní konzistence.

3.4 Prosazovat přísná opatření řízení přístupu k původním datům, maskovaným datům a klíčům pro opětovnou identifikaci.

3.5 S maskovanými nebo pseudonymizovanými datovými sadami nakládat jako s citlivými daty, na která se vztahuje protokolování přístupů, kontroly uchovávání a postupy reakce na incidenty.

3.6 Ověřovat účinnost těchto opatření prostřednictvím průběžného testování, monitorování a auditních postupů.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje tuto politiku a zajišťuje její uplatňování jako součást širších iniciativ v oblasti správy a řízení IT a ochrany dat.

4.2 Ředitel informační bezpečnosti (CISO) / manažer ISMS

4.2.1 Odpovídá za dohled nad implementací a průběžným zajišťováním souladu.

4.2.2 Zajišťuje soulad s článkem 6.1.3 normy ISO/IEC 27001 (ošetření rizik) a článkem 8.1 (provozní řízení).

4.2.3 Provádí přezkum logů a ověřuje účinnost opatření.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána nejméně jednou ročně nebo dříve v případě:

9.1.1 regulatorních změn ovlivňujících maskování nebo pseudonymizaci,

9.1.2 zavedení nových IT systémů zpracovávajících citlivá data,

9.1.3 významných změn ve schématu klasifikace dat organizace,

9.1.4 zjištění auditu indikujících nedostatky opatření,

9.1.5 vzniku nových hrozeb nebo technologií maskování.

9.2 Manažer ISMS vede přezkum po konzultaci s DPO, vlastníky dat, IT bezpečností a útvarem právní a compliance. Aktualizace musí být vedeny v režimu správy verzí, schváleny výkonným vedením a oznámeny všem dotčeným zainteresovaným stranám.

10. Související politiky a vazby

10.1 P13 - Politika klasifikace dat a označování. Rozhodnutí o maskování a pseudonymizaci jsou přímo závislá na klasifikaci datových polí a úrovních citlivosti definovaných v P13.

10.2 P14 - Politika uchovávání údajů a likvidace. Transformované datové sady musí být uchovávány a likvidovány v souladu s pravidly životního cyklu uvedenými v P14, přičemž je zajištěno, že s maskovanými a pseudonymizovanými daty je nakládáno jako s citlivými.

10.3 P17 - Politika ochrany dat a soukromí. Stanoví zásady ochrany soukromí a regulatorní východiska pro uplatnění pseudonymizace jako činnosti zpracování v souladu s GDPR a obdobnými právními předpisy.

10.4 P22 - Politika protokolování a monitorování. Umožňuje centralizovaný audit a upozorňování na události maskování a pseudonymizace v souladu se strukturovanými protokoly bezpečnostního monitorování.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 6.1.3 - Plán ošetření rizik: stanoví maskování a pseudonymizaci jako mechanismy ošetření rizik ke snížení identifikovatelnosti citlivých dat v prostředích zpracování, která nejsou nezbytná pro primární účel.

11.1.2 Článek 8.1 - Provozní plánování a řízení: vyžaduje technická a procesní opatření pro bezpečnou transformaci dat během zpracování, ukládání nebo přenosu.

11.2 ISO/IEC 27002:2022

11.2.1 Opatření 8.11, 8: pokyny pro maskování dat a pseudonymizaci za účelem minimalizace rizik opětovné identifikace a úniku dat.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PM-17 - Ochrana PII: implementace technologií zvyšujících ochranu soukromí, jako je maskování a pseudonymizace.

11.3.2 PT-2, PT-3: minimalizace a zabezpečení zpracování PII - transformace ke snížení identifikovatelnosti a vynucení řízení přístupu.

11.3.3 SC-12, SC-28, SC-30: důvěrnost a integrita dat - opatření důvěrnosti a zastření při ukládání, přenosu a používání.

11.4 GDPR (2016/679)

11.4.1 Článek 4 odst. 5: formální definice pseudonymizace.

11.4.2 Článek 32: Zabezpečení zpracování - organizační a technická opatření pro pseudonymizaci.

11.4.3 Článek 5 odst. 1 písm. c) a f): minimalizace údajů a důvěrnost s využitím pseudonymizace/maskování.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. c): vyžaduje technologie zvyšující ochranu soukromí, jako je maskování a pseudonymizace, jako bezpečnostní opatření.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 10 odst. 1: rámec řízení rizik v oblasti ICT zahrnuje opatření pro maskování a pseudonymizaci.

11.6.2 Článek 10 odst. 2 písm. e): vyžaduje používání transformačních technologií k ochraně osobních a finančních dat.

11.7 COBIT 2019

11.7.1 DSS05.01: Chránit informační aktiva - požadavky na maskování a pseudonymizaci.

11.7.2 DSS06.06: Bezpečné testování a analytika - maskování v prostředích mimo produkční prostředí.

11.7.3 MEA03: Monitorování souladu z hlediska účinnosti maskování a pseudonymizace.