					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P13S					Název dokumentu: **Politika klasifikace a označování dat**							
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	Články 5.3, 8	
ISO/IEC 27002:2022	Opatření 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU NIS2	Článek 21(2)(a)	
EU DORA	Článek 5(8)	
COBIT 2019	BAI03.05, DSS05	
GDPR	Články 5, 32	

1. Účel

1.1 Tato politika stanoví, jak musí být veškeré informace zpracovávané organizací klasifikovány a označovány, aby byla po celou dobu jejich životního cyklu zachována jejich důvěrnost, integrita a dostupnost.

1.2 Zavádí jednotný přístup k nakládání s daty tím, že informacím přiřazuje odpovídající úrovně ochrany podle jejich citlivosti, dopadu na činnost organizace nebo právních povinností.

1.3 Klasifikace a označování pomáhají snižovat riziko náhodného zpřístupnění, neoprávněného přístupu nebo nesprávného nakládání s citlivými daty, zejména v prostředí SME, které může využívat jednodušší systémy a menší počet formalizovaných kontrol.

1.4 Tato politika je zásadní pro certifikaci podle ISO/IEC 27001 a zajištění souladu s regulatorními požadavky, zejména s právními předpisy na ochranu osobních údajů, jako je GDPR, a rámci kybernetické bezpečnosti, jako jsou NIS2 a DORA.

2. Rozsah

2.1 Tato politika se vztahuje na veškerá data organizace bez ohledu na jejich formát nebo umístění, včetně:

2.1.1 elektronických dokumentů, tabulek, e-mailů, formulářů, obrázků a naskenovaných souborů,

2.1.2 fyzických dokumentů, jako jsou tištěné záznamy, zprávy, faktury a poznámky,

2.1.3 dat uložených nebo zpracovávaných v cloudových službách, na lokálních serverech, vyměnitelných médiích nebo osobních zařízeních používaných pro pracovní účely,

2.1.4 dočasných nebo přechodných dat vytvářených v průběhu provozních činností (např. logy, cache soubory, e-maily).

2.2 Tuto politiku jsou povinni dodržovat všichni zaměstnanci, dodavatelé, dočasní pracovníci a externí poskytovatelé s přístupem k datům organizace.

2.3 Politika se uplatňuje v celém životním cyklu dat — od jejich vytvoření a uložení přes přístup a přenos až po archivaci nebo výmaz.

3. Cíle

3.1 Vymezit jednoduché a vymahatelné schéma klasifikace, které lze snadno pochopit a uplatňovat v celé organizaci.

3.2 Stanovit povinnost klasifikovat každé datové aktivum podle jeho citlivosti a odpovídajícím způsobem je označit tak, aby bylo zřejmé správné nakládání, uložení a přístup.

3.3 Zajistit, aby byly postupy označování dat začleněny do pracovních procesů, jako je onboarding, zahájení projektu a konfigurace systémů.

3.4 Snižovat riziko narušení bezpečnosti dat uplatňováním opatření pro nakládání s daty (např. šifrování, omezení přístupu) podle úrovně klasifikace.

3.5 Zajistit soulad s požadavky na ochranu soukromí a bezpečnost informací tím, že bude možné doložit, že citlivá data (např. osobní, finanční nebo proprietární) jsou řádně označena a spravována.

3.6 Stanovit odpovědnost za rozhodnutí o klasifikaci a zajistit pravidelné přezkumy a aktualizace podle vývoje obchodních a právních požadavků.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Odpovídá za tuto politiku a schvaluje schéma klasifikace.

4.1.2 Zajišťuje dohled nad tím, aby odpovědnosti za klasifikaci byly řádně delegovány a vykonávány.

4.1.3 Přezkoumává a schvaluje všechny výjimky z požadavků na klasifikaci nebo označování.

4.1.4 Zajišťuje, aby postupy nakládání s daty splňovaly požadavky na soulad s právními předpisy, jako jsou GDPR a DORA.

4.2 vlastník informací / správce dat

4.2.1 Při vytvoření nebo pořízení přiřazuje každé nové datové sadě nebo informačnímu aktivu počáteční klasifikaci.

4.2.2 Zajišťuje, aby byla tam, kde je to vhodné, použita viditelná označení (např. záhlaví souborů, zápatí, vodoznaky, názvy složek).

4.2.3 Pravidelně přezkoumává klasifikaci s cílem ověřit její relevanci, správnost a případnou potřebu změny (např. po odtajnění nebo zveřejnění).

4.2.4 Spolupracuje s vedoucím IT na uplatňování technických ochranných opatření podle klasifikace (např. přístupová oprávnění, šifrování).

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

9. Požadavky na přezkum a aktualizaci

9.1 Tato politika musí být každoročně přezkoumána GM a správcem dat, aby bylo zajištěno, že odráží:

9.1.1 změny v obchodních operacích nebo typech dat,

9.1.2 nové regulatorní požadavky (např. v oblasti ochrany osobních údajů nebo finančního dohledu),

9.1.3 technologické změny ovlivňující možnosti označování nebo klasifikace.

9.2 Přezkum musí zahrnovat aktualizace kategorií klasifikace, nástrojů nebo postupů označování a obsahu školení a zvyšování povědomí.

9.3 Revize politiky musí být schváleny GM a sděleny všem pracovníkům. Pro účely auditu musí být uchovávána evidence verzí.

10. Související politiky a vazby

10.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Přiřazuje odpovědnost za vlastnictví politiky a její uplatňování.

10.2 P4S – Politika řízení přístupu: Slaďuje přístup do systémů s úrovněmi klasifikace dat.

10.3 P12S – Politika správy aktiv: Sleduje fyzická a digitální aktiva, která ukládají klasifikovaná data.

10.4 P17S – Politika ochrany dat a soukromí: Upravuje ochranu osobních údajů, z nichž velká část je klasifikována jako Důvěrná.

10.5 P30S – Politika reakce na incidenty: Definuje eskalační cesty a postupy reakce v případě porušení klasifikace nebo zpřístupnění dat.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 5.3: Vyžaduje jasně vymezené odpovědnosti za nakládání s daty a jejich ochranu.

11.1.2 Článek 8.1: Vyžaduje operativní plánování a kontroly, včetně těch, které souvisejí s klasifikací dat.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.12: Poskytuje pokyny pro klasifikaci informací na základě rizik a regulatorních požadavků.

11.2.2 Opatření 5.13: Popisuje praktické mechanismy označování a související pravidla nakládání.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: Vyžaduje označování informací tak, aby ochranná opatření odpovídala klasifikaci.

11.3.2 MP-3 / MP-5: Poskytují pokyny pro označování a řízení médií a výstupů.

11.4 GDPR

11.4.1 Články 5 a 32: Vyžadují minimalizaci údajů a zajištění integrity prostřednictvím odpovídající klasifikace a ochranných opatření při nakládání s daty.

11.5 EU NIS2

11.5.1 Článek 21(2)(a): Ukládá technická a organizační opatření pro ochranu dat na základě rizik.

11.6 EU DORA

11.6.1 Článek 5(8): Vyžaduje, aby organizace klasifikovaly datová aktiva jako součást programu řízení rizik v oblasti ICT.

11.7 COBIT 2019

11.7.1 BAI03.05: Požaduje klasifikaci informací a ochranu přiměřenou riziku.

11.7.2 DSS05.02: Zabývá se uplatňováním kontrol založených na klasifikaci a monitorováním.