					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P13					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**

1. Účel

1.1 Tato politika stanoví formální rámec pro klasifikaci a označování informačních aktiv organizace na základě jejich citlivosti, míry rizikové expozice a regulatorních povinností.

1.2 Zajišťuje, aby veškeré informace — bez ohledu na to, zda jsou ukládány, přenášeny nebo zpracovávány — byly jednoznačně kategorizovány a označeny způsobem, který vyjadřuje požadovanou úroveň ochrany a pravidla pro nakládání s nimi.

1.3 Tato politika zavádí strukturovanou klasifikaci v souladu s postupy organizace pro řízení rizik a podporuje cíle důvěrnosti, integrity a dostupnosti u digitálních i fyzických dat.

1.4 Toto opatření je nezbytné pro zajištění řízení přístupu na základě rolí, auditní připravenosti, vhodného sdílení dat a účinného nasazení technických bezpečnostních opatření, jako jsou šifrování, zálohování a monitorování.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechna informační aktiva organizace, včetně dokumentů, databází, záznamů a komunikace,

2.1.2 všechny formáty dat, včetně digitálních, tištěných, psaných nebo ústních,

2.1.3 všechna prostředí: on-premise, vzdálená, mobilní a cloudová,

2.1.4 všechny zaměstnance, smluvní pracovníky, poskytovatele služeb a externí zpracovatele, kteří vytvářejí, zpracovávají nebo ukládají informace organizace.

2.2 Rozsah zahrnuje interně vytvořený obsah, externě získaná data, osobní údaje podléhající povinnostem podle právních předpisů na ochranu soukromí (např. GDPR) a informace vyměňované s klienty, partnery a regulačními orgány.

2.3 Vztahuje se na všechny systémy používané k ukládání nebo přenosu dat, včetně podnikových aplikací, souborových serverů, e-mailových systémů, cloudových platforem a záložních úložišť.

3. Cíle

3.1 Zavést v celé organizaci standardizované schéma klasifikace založené na dopadu zpřístupnění nebo kompromitace dat.

3.2 Zajistit, aby všechny informace byly viditelně a trvale označeny tak, aby odrážely svou klasifikační úroveň a požadavky na nakládání.

3.3 Prosazovat pravidla pro nakládání s daty a řízení přístupu v souladu s klasifikací, včetně šifrování, protokolování, ochrany přenosu a plánování uchovávání.

3.4 Podporovat soulad s mezinárodními normami (ISO/IEC 27001, 27002), právními rámci (GDPR, NIS2, DORA) a interními politikami řízení rizik.

3.5 Zajistit, aby všichni uživatelé rozuměli svým odpovědnostem při ochraně dat, používání štítků a správném nakládání s klasifikovanými informacemi.

3.6 Udržovat dohledatelnost mezi stavem klasifikace, souvisejícími bezpečnostními opatřeními a evidencí aktiv organizace pro účely auditu a souladu.

4. Role a odpovědnosti

4.1 Ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za politiku klasifikace a označování informací a zajišťuje její soulad s regulatorními, smluvními a provozními požadavky.

4.1.2 Schvaluje klasifikační úrovně, standardy označování a změny této politiky.

4.1.3 Vykonává dohled nad dodržováním politiky prostřednictvím auditů, metrik a přezkumu výjimek.

4.1.4 Koordinuje meziútvarovou správu a řízení s útvary právním a compliance, ochrany osobních údajů a řízení rizik.

4.2 Vlastníci informací

4.2.1 Odpovídají za klasifikaci informačních aktiv ve své gesci podle klasifikačního schématu organizace.

4.2.2 Uplatňují klasifikační štítky při vytvoření, aktualizaci nebo převzetí informací.

4.2.3 Pravidelně přezkoumávají klasifikaci aktiv, zejména v reakci na změny citlivosti, regulatorního rozsahu nebo obchodní hodnoty.

4.2.4 Zajišťují, aby s citlivými daty bylo po celou dobu jejich životního cyklu nakládáno přiměřeně a aby byla správně označena.

[... 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 přezkoumána nejméně jednou ročně, aby byl zajištěn soulad s:

9.1.1 vyvíjejícími se regulatorními požadavky (např. GDPR, NIS2, DORA),

9.1.2 aktualizacemi pokynů pro klasifikaci podle ISO/IEC 27001 nebo 27002,

9.1.3 organizačními změnami ovlivňujícími citlivost dat nebo vlastnictví,

9.1.4 technologickými změnami, včetně nových platforem pro správu dokumentů nebo dat.

9.2 Ředitel informační bezpečnosti (CISO) zahajuje přezkum ve spolupráci s Výborem pro bezpečnost informací, právním oddělením a dotčenými útvary.

9.3 Přezkumy musí zahrnovat:

9.3.1 účinnost vynucování klasifikace a dodržování požadavků uživateli,

9.3.2 analýzu incidentů nebo výjimek souvisejících s chybnou klasifikací,

9.3.3 zpětnou vazbu uživatelů k nástrojům označování nebo podpůrným materiálům,

9.3.4 porovnání se standardy klasifikace používanými v odvětví.

9.4 Aktualizace politiky musí být vedeny v režimu správy verzí, zdokumentovány v repozitáři ISMS a komunikovány všem relevantním pracovníkům se zdůrazněním nových odpovědností nebo změn nástrojů.

9.5 Noví zaměstnanci musí být s aktuální verzí politiky seznámeni během onboardingu. Všichni zaměstnanci musí po významných změnách politiky absolvovat opakovací školení.

10. Související politiky a vazby

10.1 Tato politika je přímo podporována a vynucuje opatření popsaná v následujících souvisejících politikách:

10.1.1 P4 - Politika řízení přístupu: Přístup k informacím se řídí klasifikačními úrovněmi; citlivější data vyžadují přísnější řízení přístupu a autorizační mechanismy.

10.1.2 P11 - Politika správy uživatelských účtů a oprávnění: Posiluje přidělování oprávnění na základě principu potřeby znát, který vychází z klasifikačních stupňů.

10.1.3 P12 - Politika správy aktiv: Zajišťuje, aby každé aktivum v evidenci obsahovalo svou klasifikaci a štítek, čímž podporuje dohledatelnost a odpovědnost.

10.1.4 P14 - Politika uchovávání a likvidace dat: Pravidla uchovávání a likvidace jsou určována klasifikační úrovní dat a regulatorními požadavky na uchovávání.

10.1.5 P18 - Politika kryptografických opatření: Uplatňuje odpovídající standardy šifrování na základě klasifikace informačního aktiva.

10.1.6 P22 - Politika protokolování a monitorování: Umožňuje monitorování přístupu ke klasifikovaným informacím a jejich pohybu, zajišťuje auditovatelnost a odhalování chybného označení nebo zneužití.

10.2 Každá vazba zajišťuje konzistentní ochranu informací v celém jejich životním cyklu, od vytvoření a klasifikace až po bezpečné nakládání, ukládání, přenos a konečnou likvidaci.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými normami a regulatorními rámci upravujícími klasifikaci a označování citlivých informací.

11.2 ISO/IEC 27001

11.2.1 Článek 4.2 – Pochopení potřeb a očekávání zainteresovaných stran. Požadavky na klasifikaci často vyplývají z právních, regulatorních nebo smluvních povinností uložených zainteresovanými stranami (např. GDPR, dohody o mlčenlivosti s klienty), které se musí promítnout do této politiky.

11.2.2 Článek 6.1.3 – Ošetření rizik bezpečnosti informací. Klasifikace přímo ovlivňuje výběr opatření pro ošetření rizik, včetně řízení přístupu, šifrování a uchovávání, podle citlivosti dat.

11.2.3 Článek 7.2 – Kompetence. Tato politika stanoví povinnost školení pro pracovníky odpovědné za klasifikaci a označování, což spadá do požadavků na kompetence.

11.2.4 Článek 7.3 – Povědomí. Tato politika vyžaduje, aby si všichni uživatelé byli vědomi klasifikačních stupňů a svých odpovědností při nakládání s informacemi, čímž naplňuje povinnosti v oblasti povědomí.

11.2.5 Článek 7.5 – Dokumentované informace. Samotná politika klasifikace je řízeným dokumentem a postupy, záznamy o školení a klasifikační štítky jsou součástí dokumentovaných informací.

11.2.6 Článek 8.1 – Provozní plánování a řízení. Klasifikace a označování jsou provozní procesy začleněné do řízení životního cyklu dat a tento článek zajišťuje, že takové činnosti jsou plánovány, implementovány a řízeny.

11.2.7 Článek 9.1 – Monitorování, měření, analýza a vyhodnocování. Tato politika obsahuje ustanovení pro monitorování souladu klasifikace, trendů incidentů a účinnosti schématu označování.

11.2.8 Článek 10.1 – Neshoda a nápravné opatření. Tato politika vymezuje reakce na chybnou klasifikaci, včetně nápravných opatření, jako je opakované školení, aktualizace a ošetření výjimek.

11.3 ISO/IEC 27002:2022

11.3.1 Opatření 5.12 – Klasifikace informací. Toto opatření zajišťuje, aby byly informace klasifikovány podle své citlivosti, hodnoty a kritičnosti — přesně to tato politika formalizuje.

11.3.2 Opatření 5.13 – Označování informací. Toto opatření vyžaduje odpovídající označování informací v souladu s jejich klasifikační úrovní, což je touto politikou plně pokryto.

11.3.3 Opatření 5.10 – Přípustné užívání firemního majetku. Tato politika stanoví, jak mají uživatelé nakládat s klasifikovanými daty, a přímo tak podporuje přípustné užívání a předchází zneužití.

11.3.4 Opatření 5.11 – Vrácení aktiv. Klasifikace pomáhá zajistit, aby byla citlivá data identifikována a bezpečně vrácena nebo sanitizována při odchodu zaměstnance nebo dodavatele.

11.3.5 Opatření 5.9 – Evidence informací a dalších souvisejících aktiv. Klasifikace je často navázána na evidenci aktiv, která musí odrážet klasifikační úroveň každé položky, aby podpořila správné přiřazení opatření.

11.3.6 Opatření 5.14 – Přenos informací. Klasifikační úrovně ovlivňují opatření pro interní a externí přenosy dat (např. šifrování, schvalování, omezení přístupu).

11.3.7 Opatření 8.12 – Prevence úniku dat. Vynucování klasifikace a označování podporuje prevenci neoprávněného zpřístupnění a ztráty dat.

11.3.8 Opatření 8.11 – Maskování dat. Některé klasifikační úrovně (např. Důvěrné, Omezené) mohou vyžadovat maskování při použití dat v testovacích/vývojových prostředích nebo analytice.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 – Politika a postupy ochrany systémů a komunikace: podporuje klasifikační politiky jako součást zastřešující ochrany dat.

11.4.2 AC-16 – Bezpečnostní atributy: implementuje vynucování přístupu na základě klasifikačních metadat a oprávnění uživatelů.

11.4.3 MP-3 / MP-5 – Označování médií a ochrana při přepravě: vynucuje označování a ochranu dat v klidovém stavu i při přenosu podle klasifikace.

11.5 GDPR (2016/679)

11.5.1 Článek 5 – Zásady ochrany osobních údajů: vyžaduje, aby byly osobní údaje zpracovávány bezpečně a přiměřeně jejich citlivosti.

11.5.2 Článek 32 – Zabezpečení zpracování: posiluje klasifikaci jako mechanismus ochrany dat na základě rizik a přiměřených technických opatření.

11.6 směrnice NIS2 (2022/2555)

11.6.1 Článek 21(2)(a): vyžaduje politiky pro řízení rizik bezpečnosti informací, včetně opatření pro klasifikaci aktiv a dat.

11.6.2 Článek 21(3): podporuje přijetí opatření k vynucování odpovídajícího nakládání s daty — podpořeno označováním na základě klasifikace.

11.7 nařízení DORA (2022/2554)

11.7.1 Článek 5 – Správa a řízení a kontrola: vyžaduje rámce správy a řízení, které klasifikují datová aktiva pro účely řízení rizik v oblasti ICT.

11.7.2 Článek 9 – Řízení rizik v oblasti ICT: ukládá technická a organizační opatření pro kritická ICT aktiva, včetně klasifikace a označování.

11.8 COBIT 2019

11.8.1 DSS05.02 – Řízení bezpečnostních služeb: prosazuje klasifikaci informační bezpečnosti k zajištění ochrany podnikových dat.

11.8.2 MEA03 – Monitorování, vyhodnocování a posuzování souladu: podporuje pravidelný audit a přezkum klasifikačních postupů za účelem zajištění dodržování politiky a dosažené úrovně vyspělosti.