					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P13S					Názov dokumentu: **Politika klasifikácie a označovania údajov**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 5.3, 8	
ISO/IEC 27002:2022	Kontroly 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Smernica EÚ NIS2	Článok 21(2)(a)	
Nariadenie EÚ DORA	Článok 5(8)	
COBIT 2019	BAI03.05, DSS05.02	
Nariadenie EÚ GDPR	Články 5, 32	

1. Účel

1.1 Táto politika stanovuje, ako musia byť všetky informácie, s ktorými organizácia nakladá, klasifikované a označované tak, aby sa počas celého ich životného cyklu zachovala ich dôvernosť, integrita a dostupnosť.

1.2 Umožňuje jednotné nakladanie s údajmi tým, že informáciám priraďuje primeranú úroveň ochrany podľa ich citlivosti, dopadu na organizáciu alebo právnych povinností.

1.3 Klasifikácia a označovanie pomáhajú znižovať riziko náhodného sprístupnenia, neoprávneného prístupu alebo nesprávneho nakladania s citlivými údajmi, najmä v malých a stredných podnikoch, ktoré sa môžu spoliehať na jednoduchšie systémy a menej formalizované kontrolné mechanizmy.

1.4 Táto politika je dôležitá pre certifikáciu podľa ISO/IEC 27001 a pre súlad s regulačnými požiadavkami, najmä v oblasti ochrany údajov, ako je GDPR, a rámcov kybernetickej bezpečnosti, ako sú NIS2 a DORA.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky údaje organizácie bez ohľadu na ich formát alebo umiestnenie, vrátane:

2.1.1 elektronických dokumentov, tabuliek, e-mailov, formulárov, obrázkov a naskenovaných súborov,

2.1.2 fyzických dokumentov, ako sú tlačené záznamy, správy, faktúry a poznámky,

2.1.3 údajov uložených alebo spracúvaných v cloudových službách, na lokálnych serveroch, vymeniteľných médiách alebo na súkromných zariadeniach používaných na pracovné účely,

2.1.4 dočasných alebo prechodných údajov vytváraných počas prevádzkových činností organizácie (napr. logy, vyrovnávacia pamäť, e-maily).

2.2 Všetci zamestnanci, zmluvní pracovníci, dočasní pracovníci a externí poskytovatelia s prístupom k údajom organizácie sú povinní dodržiavať túto politiku.

2.3 Táto politika sa uplatňuje počas celého životného cyklu údajov, od ich vytvorenia a uloženia cez prístup a prenos až po archiváciu alebo výmaz.

3. Ciele

3.1 Definovať jednoduchú a uplatniteľnú klasifikačnú schému, ktorú možno v celej organizácii ľahko pochopiť a používať.

3.2 Vyžadovať, aby každé dátové aktívum bolo klasifikované podľa svojej citlivosti a primerane označené s cieľom usmerniť správne nakladanie, uchovávanie a prístup.

3.3 Zabezpečiť, aby boli postupy označovania údajov integrované do pracovných postupov organizácie, ako je nástup nových pracovníkov, spustenie projektu a konfigurácia systému.

3.4 Znížiť riziko porušenia ochrany údajov uplatňovaním kontrol pri nakladaní s údajmi (napr. šifrovanie, obmedzenie prístupu) podľa úrovne klasifikácie.

3.5 Zabezpečiť súlad s právnymi požiadavkami v oblasti ochrany súkromia a informačnej bezpečnosti tým, že organizácia preukáže, že citlivé údaje (napr. osobné, finančné alebo proprietárne) sú riadne označené a spravované.

3.6 Zaviesť zodpovednosť za rozhodnutia o klasifikácii a zabezpečiť pravidelné preskúmavanie a aktualizáciu podľa vývoja prevádzkových a právnych potrieb.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Je vlastníkom tejto politiky a schvaľuje klasifikačnú schému.

4.1.2 Vykonáva dohľad nad tým, aby boli zodpovednosti za klasifikáciu pridelené a uplatňované.

4.1.3 Schvaľuje všetky výnimky z požiadaviek na klasifikáciu alebo označovanie.

4.1.4 Zabezpečuje, aby postupy nakladania s údajmi spĺňali požiadavky súladu podľa právnych predpisov, ako sú GDPR a DORA.

4.2 Vlastník informácií / správca údajov

4.2.1 Pri vytvorení alebo získaní každého nového súboru údajov alebo informačného aktíva priraďuje počiatočnú klasifikáciu.

4.2.2 Zabezpečuje, aby sa tam, kde je to relevantné, používali viditeľné označenia (napr. hlavičky dokumentov, päty, vodoznaky, názvy priečinkov).

4.2.3 Pravidelne preskúmava klasifikáciu s cieľom overiť jej relevantnosť, presnosť a potrebu zmien (napr. po znížení stupňa klasifikácie alebo zverejnení).

4.2.4 Spolupracuje s vedúcim IT pri uplatňovaní technických ochranných opatrení podľa klasifikácie (napr. prístupové práva, šifrovanie).

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Túto politiku musia GM a správca údajov preskúmať každoročne, aby sa zabezpečilo, že zohľadňuje:

9.1.1 zmeny v prevádzke organizácie alebo v typoch údajov,

9.1.2 nové regulačné požiadavky (napr. v oblasti ochrany údajov alebo finančného dohľadu),

9.1.3 technologické zmeny ovplyvňujúce možnosti označovania alebo klasifikácie.

9.2 Preskúmanie musí zahŕňať aktualizácie klasifikačných kategórií, nástrojov alebo postupov označovania a obsahu školení a zvyšovania povedomia.

9.3 Revízie politiky musí schváliť GM a musia byť oznámené všetkým pracovníkom. Na účely auditu sa musí uchovávať evidencia verzií.

10. Súvisiace politiky a väzby

10.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: priraďuje zodpovednosť za vlastníctvo politiky a jej uplatňovanie.

10.2 P4S – Politika riadenia prístupu: zosúlaďuje prístup do systémov s úrovňami klasifikácie údajov.

10.3 P12S – Politika správy aktív: eviduje fyzické a digitálne aktíva, na ktorých sú uložené klasifikované údaje.

10.4 P17S – Politika ochrany údajov a súkromia: upravuje ochranu osobných údajov, z ktorých mnohé sú klasifikované ako Dôverné.

10.5 P30S – Politika reakcie na incidenty: definuje eskalačné postupy a postupy reakcie pri porušení pravidiel klasifikácie alebo pri sprístupnení údajov.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.3: vyžaduje jasne vymedzené zodpovednosti za nakladanie s údajmi a ich ochranu.

11.1.2 Kapitola 8.1: vyžaduje prevádzkové plánovanie a riadenie vrátane kontrol naviazaných na klasifikáciu údajov.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.12: poskytuje usmernenie ku klasifikácii informácií na základe rizík a regulačných požiadaviek.

11.2.2 Kontrola 5.13: uvádza praktické mechanizmy označovania a súvisiace pravidlá nakladania.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: vyžaduje označovanie informácií tak, aby boli ochranné opatrenia v súlade s klasifikáciou.

11.3.2 MP-3 / MP-5: poskytujú usmernenie pre označovanie a kontrolu médií a výstupov.

11.4 Nariadenie EÚ GDPR

11.4.1 Články 5 a 32: vyžadujú minimalizáciu údajov a integritu prostredníctvom primeranej klasifikácie a ochranných opatrení pri nakladaní s údajmi.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(a): vyžaduje technické a organizačné opatrenia na ochranu údajov založené na riziku.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 5(8): vyžaduje, aby organizácie klasifikovali dátové aktíva ako súčasť programu riadenia IKT rizík.

11.7 COBIT 2019

11.7.1 BAI03.05: vyžaduje klasifikáciu informácií a ochranu primeranú riziku.

11.7.2 DSS05.02: upravuje uplatňovanie kontrol založených na klasifikácii a monitorovanie.