					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P13					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**

Právne upozornenie (autorské práva a obmedzenia používania)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševným vlastníctvom spoločnosti Clarysec LLC. Žiadna časť tohto dokumentu nesmie byť bez predchádzajúceho výslovného písomného súhlasu kopírovaná, znovu použitá, distribuovaná ani upravovaná na komerčné alebo implementačné účely.
Neoprávnené použitie je prísne zakázané a môže viesť k právnym krokom.
V prípade licencovania kontaktujte: info@clarysec.com

1. Účel

1.1 Táto politika stanovuje formálny rámec pre klasifikáciu a označovanie informačných aktív organizácie na základe ich citlivosti, rizikovej expozície a právnych povinností.

1.2 Zabezpečuje, aby všetky informácie — bez ohľadu na to, či sú uchovávané, prenášané alebo spracúvané — boli jednoznačne klasifikované a označené spôsobom, ktorý vyjadruje požadovanú úroveň ich ochrany a pravidlá nakladania s nimi.

1.3 Táto politika vyžaduje štruktúrovanú klasifikáciu zosúladenú s postupmi riadenia rizík organizácie a podporuje ciele dôvernosti, integrity a dostupnosti pri digitálnych aj fyzických typoch údajov.

1.4 Táto kontrola je nevyhnutná na umožnenie prístupu na základe rolí, pripravenosti na audit, primeraného zdieľania údajov a účinného nasadenia technických bezpečnostných opatrení, ako sú šifrovanie, zálohovanie a monitorovanie.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky informačné aktíva organizácie vrátane dokumentov, databáz, záznamov a komunikácie,

2.1.2 všetky formáty údajov vrátane digitálnych, tlačených, písomných a ústnych,

2.1.3 všetky prostredia: on-premise, vzdialené, mobilné a cloudové,

2.1.4 všetkých zamestnancov, zmluvných pracovníkov, poskytovateľov služieb a spracovateľov tretích strán, ktorí vytvárajú, spracúvajú alebo uchovávajú informácie organizácie.

2.2 Rozsah zahŕňa interne vytvorený obsah, externe získané údaje, osobné údaje podliehajúce povinnostiam podľa právnych predpisov na ochranu súkromia (napr. GDPR) a informácie vymieňané s klientmi, partnermi a regulačnými orgánmi.

2.3 Vzťahuje sa na všetky systémy používané na uchovávanie alebo prenos údajov vrátane podnikových aplikácií, súborových serverov, e-mailových systémov, cloudových platforiem a záložných úložísk.

3. Ciele

3.1 Zaviesť v celej organizácii štandardizovanú klasifikačnú schému založenú na dopade sprístupnenia alebo kompromitácie údajov.

3.2 Zabezpečiť, aby všetky informácie boli viditeľne a trvalo označené tak, aby odrážali úroveň klasifikácie a požiadavky na nakladanie.

3.3 Uplatňovať kontroly nakladania s údajmi a riadenie prístupu v súlade s klasifikáciou vrátane šifrovania, logovania, ochrany prenosu a stanovenia lehôt uchovávania.

3.4 Podporovať súlad s medzinárodnými normami (ISO/IEC 27001, 27002), právnymi rámcami (GDPR, NIS2, DORA) a internými politikami riadenia rizík.

3.5 Zabezpečiť, aby všetci používatelia rozumeli svojim povinnostiam pri ochrane údajov, uplatňovaní označení a správnom nakladaní s klasifikovanými informáciami.

3.6 Udržiavať sledovateľnosť medzi stavom klasifikácie, súvisiacimi kontrolami a inventárom aktív organizácie na účely auditu a preukazovania súladu.

4. Roly a zodpovednosti

4.1 riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za politiku klasifikácie a označovania informácií a zabezpečuje jej súlad s regulačnými, zmluvnými a prevádzkovými požiadavkami.

4.1.2 Schvaľuje úrovne klasifikácie, štandardy označovania a revízie politiky.

4.1.3 Vykonáva dohľad nad dodržiavaním politiky prostredníctvom auditov, metrík a preskúmania výnimiek.

4.1.4 Koordinuje priečnu spoluprácu s tímami pre právne záležitosti, ochranu osobných údajov a riadenie rizík.

4.2 Vlastníci informácií

4.2.1 Zodpovedajú za klasifikáciu informačných aktív vo svojej pôsobnosti podľa klasifikačnej schémy organizácie.

4.2.2 Uplatňujú klasifikačné označenia pri vytvorení, aktualizácii alebo prevzatí informácií.

4.2.3 Pravidelne preskúmavajú klasifikáciu aktív, najmä v reakcii na zmeny citlivosti, regulačného rozsahu alebo hodnoty pre organizáciu.

4.2.4 Zabezpečujú, aby sa s citlivými údajmi počas celého ich životného cyklu primerane nakladalo a aby boli správne označené.

[... 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 Táto politika sa musí preskúmavať najmenej raz ročne s cieľom zabezpečiť súlad s:

9.1.1 vyvíjajúcimi sa regulačnými požiadavkami (napr. GDPR, NIS2, DORA),

9.1.2 aktualizáciami usmernení ISO/IEC 27001 alebo 27002 ku klasifikácii,

9.1.3 organizačnými zmenami ovplyvňujúcimi citlivosť údajov alebo vlastníctvo,

9.1.4 technologickými zmenami vrátane nových platforiem na správu dokumentov alebo údajov.

9.2 riaditeľ informačnej bezpečnosti (CISO) musí iniciovať preskúmanie v spolupráci s Výborom pre informačnú bezpečnosť, právnym poradcom a dotknutými organizačnými útvarmi.

9.3 Preskúmania musia zahŕňať:

9.3.1 účinnosť presadzovania klasifikácie a mieru dodržiavania používateľmi,

9.3.2 analýzu incidentov alebo výnimiek súvisiacich s nesprávnou klasifikáciou,

9.3.3 spätnú väzbu používateľov k nástrojom označovania alebo usmerňujúcim materiálom,

9.3.4 porovnanie s odvetvovými štandardmi klasifikácie.

9.4 Aktualizácie politiky musia podliehať riadeniu verzií, byť zdokumentované v úložisku ISMS a komunikované všetkým relevantným osobám s dôrazom na nové zodpovednosti alebo zmeny nástrojov.

9.5 Noví zamestnanci musia byť počas onboardingu oboznámení s aktuálnou verziou politiky. Všetci zamestnanci musia po významných zmenách politiky absolvovať pravidelné opakovacie školenie.

10. Súvisiace politiky a väzby

10.1 Táto politika je priamo podporovaná a presadzuje kontroly opísané v nasledujúcich súvisiacich politikách:

10.1.1 P4 - Politika riadenia prístupu: Prístup k informáciám sa riadi podľa úrovní klasifikácie; citlivejšie údaje vyžadujú prísnejšie riadenie prístupu a autorizačné mechanizmy.

10.1.2 P11 - Politika správy používateľských účtov a oprávnení: Posilňuje prideľovanie oprávnení na základe zásady potreby vedieť, ktorá vychádza z klasifikačných stupňov.

10.1.3 P12 - Politika správy aktív: Zabezpečuje, aby každé aktívum v inventári obsahovalo svoju klasifikáciu a označenie, čím podporuje sledovateľnosť a priradenie zodpovednosti.

10.1.4 P14 - Politika uchovávania a likvidácie údajov: Pravidlá likvidácie a uchovávania sa určujú podľa úrovne klasifikácie údajov a regulačných požiadaviek na uchovávanie.

10.1.5 P18 - Politika kryptografických kontrol: Uplatňuje primerané štandardy šifrovania podľa klasifikácie informačného aktíva.

10.1.6 P22 - Politika logovania a monitorovania: Umožňuje monitorovanie prístupu ku klasifikovaným informáciám a ich pohybu, čím zabezpečuje auditovateľnosť a detekciu nesprávneho označenia alebo zneužitia.

10.2 Každá väzba zabezpečuje konzistentnú ochranu informácií počas celého ich životného cyklu, od vytvorenia a klasifikácie až po bezpečné nakladanie, uchovávanie, prenos a konečné zničenie.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými normami a regulačnými rámcami upravujúcimi klasifikáciu a označovanie citlivých informácií.

11.2 ISO/IEC 27001

11.2.1 Kapitola 4.2 - Pochopenie potrieb a očakávaní zainteresovaných strán. Požiadavky na klasifikáciu často vyplývajú z právnych, regulačných alebo zmluvných povinností uložených zainteresovanými stranami (napr. GDPR, klientské dohody o mlčanlivosti), ktoré musia byť zohľadnené v politike.

11.2.2 Kapitola 6.1.3 - Ošetrenie rizík informačnej bezpečnosti. Klasifikácia priamo ovplyvňuje výber opatrení na ošetrenie rizík vrátane riadenia prístupu, šifrovania a uchovávania podľa citlivosti údajov.

11.2.3 Kapitola 7.2 - Kompetencie. Politika vyžaduje, aby personál zodpovedný za klasifikáciu a označovanie bol vyškolený, čo patrí do požiadaviek na kompetencie.

11.2.4 Kapitola 7.3 - Povedomie. Politika vyžaduje, aby si všetci používatelia boli vedomí klasifikačných stupňov a svojich povinností pri nakladaní s informáciami, čím sa zosúlaďuje s požiadavkami na povedomie.

11.2.5 Kapitola 7.5 - Dokumentované informácie. Samotná politika klasifikácie je riadený dokument a postupy, záznamy o školeniach a klasifikačné označenia tvoria súčasť dokumentovaných informácií.

11.2.6 Kapitola 8.1 - Prevádzkové plánovanie a riadenie. Klasifikácia a označovanie sú prevádzkové procesy začlenené do riadenia životného cyklu údajov a táto kapitola zabezpečuje, aby takéto činnosti boli plánované, implementované a riadené.

11.2.7 Kapitola 9.1 - Monitorovanie, meranie, analýza a hodnotenie. Politika obsahuje ustanovenia na monitorovanie dodržiavania klasifikácie, trendov incidentov a účinnosti schémy označovania.

11.2.8 Kapitola 10.1 - Nezhoda a nápravné opatrenie. Politika definuje reakcie na nesprávnu klasifikáciu vrátane nápravných opatrení, ako sú opätovné školenie, aktualizácie a ošetrenie výnimiek.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrola 5.12 - Klasifikácia informácií. Táto kontrola zabezpečuje, aby boli informácie klasifikované podľa svojej citlivosti, hodnoty a kritickosti — presne to táto politika formalizuje.

11.3.2 Kontrola 5.13 - Označovanie informácií. Táto kontrola vyžaduje primerané označovanie informácií v súlade s ich úrovňou klasifikácie, čo je touto politikou plne pokryté.

11.3.3 Kontrola 5.10 - Prípustné používanie informačných a iných súvisiacich aktív. Politika určuje, ako majú používatelia nakladať s klasifikovanými údajmi, čím priamo podporuje prípustné používanie a predchádza zneužitiu.

11.3.4 Kontrola 5.11 - Vrátenie aktív. Klasifikácia pomáha zabezpečiť, aby boli citlivé údaje identifikované a bezpečne vrátené alebo sanitizované pri odchode zamestnanca alebo dodávateľa.

11.3.5 Kontrola 5.9 - Inventarizácia informácií a iných súvisiacich aktív. Klasifikácia je často prepojená s inventarizáciou aktív, ktorá musí odrážať úroveň klasifikácie každej položky na podporu správneho priradenia kontrol.

11.3.6 Kontrola 5.14 - Prenos informácií. Úrovne klasifikácie ovplyvňujú kontroly interných a externých prenosov údajov (napr. šifrovanie, schválenie, obmedzenia prístupu).

11.3.7 Kontrola 8.12 - Prevencia úniku údajov. Uplatňovanie klasifikácie a označovania podporuje predchádzanie neoprávnenému sprístupneniu a strate údajov.

11.3.8 Kontrola 8.11 - Maskovanie údajov. Určité úrovne klasifikácie (napr. Dôverné, Obmedzené) môžu vyžadovať maskovanie pri použití údajov v testovacom alebo vývojovom prostredí alebo pri analytike.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Politika a postupy ochrany systémov a komunikácie: podporuje politiky klasifikácie ako súčasť zastrešujúcej ochrany údajov.

11.4.2 AC-16 - Bezpečnostné atribúty: implementuje presadzovanie prístupu na základe klasifikačných metadát a používateľských oprávnení.

11.4.3 MP-3 / MP-5 - Označovanie médií a ochrana pri preprave: presadzuje označovanie a ochranu údajov v pokoji a pri prenose podľa klasifikácie.

11.5 Nariadenie EÚ GDPR (2016/679)

11.5.1 Článok 5 - Zásady ochrany údajov: vyžaduje, aby sa osobné údaje spracúvali bezpečne a primerane ich citlivosti.

11.5.2 Článok 32 - Bezpečnosť spracúvania: posilňuje klasifikáciu ako mechanizmus ochrany údajov založenej na riziku a primeraných technických opatreniach.

11.6 Smernica EÚ NIS2 (2022/2555)

11.6.1 Článok 21(2)(a): vyžaduje politiky riadenia rizík informačnej bezpečnosti vrátane kontrol klasifikácie aktív a údajov.

11.6.2 Článok 21(3): podporuje prijatie opatrení na presadzovanie primeraného nakladania s údajmi, podporeného označovaním na základe klasifikácie.

11.7 Nariadenie EÚ DORA (2022/2554)

11.7.1 Článok 5 - Správa a riadenie a kontrola: vyžaduje rámce správy a riadenia, ktoré klasifikujú dátové aktíva na účely riadenia rizík IKT.

11.7.2 Článok 9 - Riadenie rizík IKT: ukladá technické a organizačné opatrenia pre kritické aktíva IKT vrátane klasifikácie a označovania.

11.8 COBIT 2019

11.8.1 DSS05.02 - Riadenie bezpečnostných služieb: presadzuje klasifikáciu informačnej bezpečnosti s cieľom zabezpečiť ochranu podnikových údajov.

11.8.2 MEA03 - Monitorovanie, hodnotenie a posudzovanie súladu: podporuje pravidelný audit a preskúmanie klasifikačných postupov s cieľom zabezpečiť dodržiavanie politiky a primeranú úroveň vyspelosti.