					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P12					Názov dokumentu: **Politika správy aktív**							
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**

1. Účel

1.1 Táto politika stanovuje záväzné organizačné požiadavky na identifikáciu, klasifikáciu, správu a ochranu informačných aktív počas celého ich životného cyklu. Podporuje správu a riadenie hardvérových, softvérových, dátových, cloudových a nehmotných informačných aktív vrátane mobilných prostredí, práce na diaľku a prostredí spravovaných tretími stranami.

1.2 Účelom tejto politiky je zabezpečiť úplný prehľad o prostredí informačných aktív organizácie, aby bolo možné uplatňovať účinné bezpečnostné opatrenia, priraďovať vlastníctvo, zabezpečiť súlad a riadne vyradenie alebo likvidáciu aktív.

1.3 Táto politika je v súlade s prílohou A.5.9 normy ISO/IEC 27001:2022 tým, že vyžaduje vedenie centralizovanej evidencie informácií a súvisiacich aktív. Zabezpečuje preukázateľnú zodpovednosť tým, že každé aktívum prepája s jeho vlastníkom a uplatňuje ochranu podľa klasifikácie vychádzajúcej z citlivosti pre organizáciu a regulačných požiadaviek.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných pracovníkov, dodávateľov tretích strán a poskytovateľov služieb, ktorí spravujú, používajú, pristupujú k informačným aktívam vo vlastníctve alebo pod kontrolou organizácie alebo ich ukladajú či spracúvajú.

2.2 Rozsah zahŕňa všetky kategórie aktív, najmä:

2.2.1 Fyzické aktíva: notebooky, stolové počítače, mobilné zariadenia, vymeniteľné médiá, tlačiarne, sieťové zariadenia

2.2.2 Digitálne aktíva: softvér, aplikácie, obrazy systémov, databázy, zálohované údaje, šifrovacie kľúče

2.2.3 Informačné aktíva: štruktúrované a neštruktúrované údaje, správy, e-maily, duševné vlastníctvo

2.2.4 Cloudové a virtuálne aktíva: prostredia IaaS, SaaS, PaaS, virtuálne stroje, kontajnery

2.2.5 Logické aktíva: názvy domén, licencie, používateľské účty, referenčné konfigurácie

2.3 Táto politika upravuje aj aktíva používané pri práci na diaľku, v hybridnom režime alebo v outsourcovaných prostrediach a zabezpečuje ich ochranu a viditeľnosť aj vtedy, keď sa aktíva fyzicky nenachádzajú v priestoroch organizácie.

3. Ciele

3.1 Udržiavať úplnú, presnú a aktuálnu inventarizáciu všetkých informačných aktív organizácie s určeným vlastníctvom, klasifikáciou a údajom o umiestnení.

3.2 Určiť vlastníkov aktív zodpovedných za klasifikáciu, nakladanie s aktívami a ochranu aktív pod ich kontrolou v súlade so správou údajov a bezpečnostnými politikami.

3.3 Uplatňovať primeranú klasifikáciu a označovanie všetkých aktív podľa citlivosti, kritickosti a regulačných požiadaviek.

3.4 Chrániť aktíva podľa ich klasifikácie a súvisiacej miery vystavenia riziku vrátane uchovávania, prístupu, prenosu a likvidácie.

3.5 Presadzovať postupy vrátenia aktív a ich bezpečného vyradenia pri ukončení pracovného pomeru, ukončení zmluvného vzťahu alebo na konci životného cyklu aktíva.

3.6 Podporovať súlad s rámcami, ako sú ISO/IEC 27001, GDPR, NIS2, DORA a COBIT 2019, prostredníctvom štruktúrovanej správy aktív a auditovateľnosti.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje Politiku správy aktív a zabezpečuje pridelenie zdrojov na jej úplné zavedenie.

4.1.2 Nesie konečnú zodpovednosť za to, aby boli aktíva organizácie chránené a spravované v súlade s regulačnými a zmluvnými povinnosťami.

4.2 Riaditeľ informačnej bezpečnosti (CISO)

4.2.1 Je vlastníkom Politiky správy aktív a zabezpečuje jej integráciu do širšieho systému manažérstva informačnej bezpečnosti (ISMS) organizácie.

4.2.2 Preskúmava výnimky a odchýlky od tejto politiky a presadzuje stratégie zmierňovania založené na riziku.

4.2.3 Dohliada na pravidelné audity klasifikácie aktív, integrity inventára a súladu s požiadavkami životného cyklu aktív.

[... 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 preskúmať najmenej raz ročne alebo v reakcii na:

9.1.1 zmeny zákonných alebo regulačných povinností ovplyvňujúcich klasifikáciu aktív alebo požiadavky na evidenciu

9.1.2 zavedenie nových kategórií aktív alebo platforiem ich správy (napr. cloud-native CMDB)

9.1.3 auditné zistenia interného auditu alebo bezpečnostné incidenty súvisiace s nesprávnou správou aktív

9.1.4 organizačné zmeny ovplyvňujúce vlastníctvo alebo kontroly životného cyklu

9.2 Proces preskúmania iniciuje manažér IT aktív a koordinuje ho s CISO, obstarávaním, právnym oddelením a dotknutými vedúcimi oddelení.

9.3 Mimoriadne preskúmania môžu byť vyvolané aj:

9.3.1 akvizíciou alebo odpredajom organizačných jednotiek

9.3.2 zmenami dodávateľov ovplyvňujúcimi aktíva spravované tretími stranami

9.3.3 obnovou technológií zahŕňajúcou hromadné vyradenie alebo zriaďovanie

9.4 Všetky revízie tejto politiky musia:

9.4.1 podliehať riadeniu verzií a byť uložené v úložisku ISMS

9.4.2 byť schválené vrcholovým manažmentom

9.4.3 obsahovať zhrnutie zmien a ich odôvodnenie

9.4.4 byť oznámené všetkým dotknutým zainteresovaným stranám vrátane aktualizovaných postupov alebo školení k systémom, ak je to relevantné

10. Súvisiace politiky a väzby

10.1 Táto politika sa uplatňuje spolu s nasledujúcimi súvisiacimi politikami a podporuje ich dodržiavanie:

10.1.1 P4 - Politika riadenia prístupu: Zabezpečuje, aby viditeľnosť aktív bola zosúladená s prístupovými oprávneniami a kontrolnými mechanizmami naprieč systémami a dátovými prostrediami.

10.1.2 P7 - Politika nástupu a ukončenia: Upravuje včasné zriaďovanie a vrátenie fyzických a logických aktív počas personálnych zmien.

10.1.3 P13 - Politika klasifikácie a označovania údajov: Stanovuje záväzné pravidlá klasifikácie aktív, ktoré určujú označovanie, nakladanie a likvidáciu.

10.1.4 P14 - Politika uchovávania a likvidácie údajov: Vymedzuje lehoty a metódy bezpečnej likvidácie digitálnych a fyzických aktív obsahujúcich informácie.

10.1.5 P22 - Politika protokolovania a monitorovania: Umožňuje sledovateľnosť prístupu k aktívam a ich používania prostredníctvom systémového protokolovania, viditeľnosti koncových bodov a behaviorálnej analytiky.

10.1.6 P30 - Politika reakcie na incidenty: Podporuje rýchle zamedzenie šírenia a vyšetrovanie incidentov súvisiacich s aktívami, ako sú stratené notebooky alebo nesledované úložné médiá.

10.2 Tieto politiky tvoria ucelenú štruktúru správy a riadenia, ktorá zabezpečuje, že aktíva sú bezpečne spravované, presne evidované a primerane spracúvané počas celého životného cyklu.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými normami informačnej bezpečnosti a regulačnými rámcami, ktoré vyžadujú dôslednú správu aktív počas celého životného cyklu.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 8.1 – Vyžaduje, aby organizácie plánovali, implementovali a riadili procesy potrebné na splnenie požiadaviek informačnej bezpečnosti vrátane požiadaviek na riadenie životného cyklu aktív.

11.3 ISO/IEC 27002:2022 – Kontroly 5.9 až 5.11

11.3.1 Kapitola 5.9 – Inventár informácií a ďalších súvisiacich aktív: Vyžaduje aktuálnu a úplnú evidenciu všetkých aktív relevantných pre spracúvanie informácií.

11.3.2 Kapitola 5.10 – Prípustné používanie informácií a aktív: Podporené pravidlami používania, vlastníctvom a procesmi vrátenia.

11.3.3 Kapitola 5.11 – Vrátenie aktív: Implementované prostredníctvom formálnych postupov odovzdania a vyradenia.

11.3.4 Tieto kontroly stanovujú štruktúrované požiadavky na identifikáciu, označovanie, udržiavanie a sledovanie aktív organizácie spolu so zodpovednosťami vlastníkov a správcov počas celého životného cyklu.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 – Inventár komponentov systému: Premietnuté do centralizovanej správy aktív, viditeľnosti v reálnom čase a prepojenia na prevádzkové konfigurácie.

11.4.2 RA-3 – Posúdenie rizík: Evidencia aktív slúži ako základný prvok modelovania hrozieb a hodnotenia rizík.

11.4.3 MP-6 – Sanitácia médií: Uplatňovaná prostredníctvom bezpečných metód likvidácie definovaných v kontrolách životného cyklu aktív a v Politike likvidácie údajov.

11.5 Nariadenie EÚ GDPR (2016/679):

11.5.1 Článok 30 – Záznamy o spracovateľských činnostiach: Vyžaduje, aby organizácie dokumentovali systémy, zariadenia a úložiská, ktoré uchovávajú alebo spracúvajú osobné údaje.

11.5.2 Článok 32 – Bezpečnosť spracúvania: Zodpovedá hodnoteniu rizík na základe aktív a ochranným opatreniam prispôsobeným klasifikovaným aktívam a kritickej infraštruktúre.

11.6 Smernica EÚ NIS2 (2022/2555):

11.6.1 Článok 21(2)(a, b): Vyžaduje viditeľnosť aktív a ich evidenciu ako základ pre analýzu rizík, ochranu a reakciu na incidenty kybernetickej bezpečnosti.

11.6.2 Článok 21(3): Zdôrazňuje nevyhnutnosť štruktúrovanej správy aktív ako súčasti bezpečnostnej kultúry organizácie.

11.7 Nariadenie EÚ DORA (2022/2554):

11.7.1 Článok 5 – Správa a riadenie IKT a vnútorná kontrola: Vyžaduje, aby finančné subjekty riadili aktíva IKT s jasne definovanou evidenciou, vlastníctvom a požiadavkami na ochranu.

11.7.2 Článok 9 – Rámec riadenia rizík IKT: Stanovuje, že procesy správy aktív musia podporovať zmierňovanie hrozieb, plánovanie kontinuity činností a odolnosť služieb.

11.8 COBIT 2019:

11.8.1 BAI09 – Správa aktív: Priamo zosúladené so štruktúrovanou identifikáciou, klasifikáciou, používaním a likvidáciou podnikových aktív.

11.8.2 DSS01 – Riadené prevádzkové činnosti: Podporuje implementáciu opatrení, ktoré zabezpečujú ochranu aktív a nepretržitú prevádzkovú správu a riadenie.

11.8.3 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: Zabezpečuje pravidelný audit kontrol správy aktív a ich účinnosti vo vzťahu k regulačnému súladu.