					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P12S					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Požiadavky na správu aktív
ISO/IEC 27002:2022	Kontrola 5	Kontroly správy aktív
NIST SP 800-53 Rev.5	CM-8	Inventarizácia systémových komponentov
Smernica EÚ NIS2	Článok 21(2)(a)	Evidencia aktív na ochranu sietí a informačných systémov
Nariadenie EÚ DORA	Článok 5(8)	Požiadavky na inventarizáciu aktív IKT
COBIT 2019	BAI	Riadenie životného cyklu IT aktív
Nariadenie EÚ GDPR	Článok 30	Záznamy o spracovateľských činnostiach

1. Účel

1.1 Táto politika stanovuje spôsob, akým organizácia identifikuje, eviduje, chráni a vyraďuje svoje informačné aktíva vrátane fyzických aj digitálnych súčastí.

1.2 Cieľom je znížiť prevádzkové a bezpečnostné riziká zabezpečením prehľadu o aktívach, priradením zodpovednosti a bezpečným nakladaním so všetkými aktívami organizácie počas celého ich životného cyklu.

1.3 Spoľahlivá inventarizácia aktív podporuje plnenie regulačných požiadaviek, reakciu na incidenty, plánovanie kontinuity činností a riadenie rizík.

1.4 Táto politika zároveň podporuje certifikáciu podľa ISO/IEC 27001 a preukazuje súlad so zákonnými, finančnými a kybernetickobezpečnostnými povinnosťami podľa rámcov, ako sú GDPR, NIS2 a DORA.

1.5 Pre malé a stredné podniky (SME) je jednoduchý, ale systematický prístup k správe aktív nevyhnutný na predchádzanie nespravovaným zariadeniam, únikom údajov alebo zisteniam pri audite, najmä pri obmedzených personálnych a technických kapacitách.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky aktíva vo vlastníctve organizácie, prenajaté organizáciou alebo inak spravované organizáciou vrátane aktív používaných pri:

2.1.1 práci v kancelárii

2.1.2 práci na diaľku alebo v hybridnom režime

2.1.3 terénnych alebo mobilných činnostiach

2.1.4 činnostiach v cloudovom prostredí a v outsourcovanom prostredí

2.2 Medzi zahrnuté typy aktív patria okrem iného:

2.2.1 Hardvér: notebooky, stolové počítače, monitory, telefóny, tablety, USB disky, smerovače, tlačiarne, zálohovacie médiá

2.2.2 Softvér: nainštalované aplikácie, SaaS služby, operačné systémy, antivírusový softvér, licencie

2.2.3 Dátové aktíva: úložiská podnikových údajov, tabuľkové prehľady, záznamy o zákazníkoch, zdrojový kód

2.2.4 Digitálne poverenia a služby: názvy domén, digitálne certifikáty, API kľúče, e-mailové účty, cloudové prístupové údaje

2.2.5 Prístupové prostriedky: kľúče, čipové karty, prístupové prívesky, biometrické tokeny

2.3 Do rozsahu tejto politiky patria všetci zamestnanci, zmluvní pracovníci a poskytovatelia tretích strán, ktorí nakladajú s aktívami organizácie.

2.4 Politika upravuje krátkodobé aktíva (napr. notebooky pre konkrétny projekt) aj dlhodobé aktíva, ako aj zdieľané aktíva používané viacerými pracovníkmi.

3. Ciele

3.1 Zaviesť a udržiavať úplnú a presnú inventarizáciu všetkých relevantných aktív, ktorá sa priebežne aktualizuje.

3.2 Zabezpečiť, aby každé aktívum malo určeného vlastníka zodpovedného za jeho používanie, uchovávanie a vrátenie.

3.3 Klasifikovať aktíva podľa citlivosti, dopadu na organizáciu alebo regulačnej relevantnosti tak, aby bolo možné uplatniť primeranú úroveň ochrany.

3.4 Stanoviť jasné postupy pre vydávanie aktív, ich opätovné pridelenie, údržbu, nahlasovanie straty a vyradenie.

3.5 Zabezpečiť bezpečné nakladanie s aktívami počas celého ich životného cyklu a zabezpečiť, aby informácie, ktoré obsahujú, boli pri likvidácii chránené alebo bezpečne vymazané.

3.6 Znížiť pravdepodobnosť bezpečnostných incidentov spôsobených neevidovanými, nevrátenými alebo nesprávne používanými zdrojmi organizácie.

3.7 Podporiť súlad s príslušnými právnymi predpismi (napr. zásadou zodpovednosti podľa GDPR) a normami kybernetickej bezpečnosti relevantnými pre certifikáciu.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Je vlastníkom tejto politiky a zodpovedá za to, aby sa postupy správy aktív zaviedli a dodržiavali v celej organizácii.

4.1.2 Preskúmava a schvaľuje aktualizácie inventarizácie aktív a podľa potreby povoľuje vyradenie alebo prevod aktív.

4.1.3 Musí byť informovaný o každej významnej strate, krádeži alebo zneužití aktív.

4.2 IT vedúci alebo určený správca aktív

4.2.1 Udržiava inventarizáciu aktív (napr. v tabuľkovom prehľade, tiketovacom systéme alebo jednoduchom nástroji na evidenciu aktív).

4.2.2 Priraďuje vlastníctvo aktív a sleduje zmeny ich stavu (napr. nové, používané, v oprave, vyradené).

4.2.3 Overuje, že všetky vydané aktíva sú zdokumentované a prepojené s konkrétnou osobou alebo organizačnou jednotkou.

4.2.4 Zabezpečuje, aby sa klasifikačné označenia uplatňovali a dodržiavali (napr. interné použitie, Dôverné).

4.2.5 Koordinuje prevzatie, sanitizáciu a deaktiváciu aktív počas offboardingu alebo vyradenia.

4.2.6 Oznamuje všetky nevyriešené nezrovnalosti v evidencii aktív GM.

[... 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 a vždy, keď:

9.1.1 sa zavedú nové typy technológií alebo aktív

9.1.2 sa zmenia postupy evidencie aktív (napr. zavedením nových nástrojov alebo platforiem)

9.1.3 nové regulačné povinnosti ovplyvnia sledovateľnosť aktív alebo ich likvidáciu

9.1.4 incident alebo audit identifikuje medzeru v súčasných postupoch správy aktív

9.2 Preskúmania musia zahŕňať GM a IT vedúceho a musia obsahovať aktualizácie postupov nakladania s aktívami, šablón inventarizácie a pokynov ku klasifikácii.

9.3 Všetky aktualizácie musia byť zdokumentované a oznámené dotknutým pracovníkom. Musí sa uchovávať zoznam zmien podliehajúci správe verzií.

10. Súvisiace politiky a väzby

10.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: priraďuje zodpovednosť za vlastníctvo politík a IT prevádzku.

10.2 P4S – Politika riadenia prístupu: prepája používanie aktív (napr. notebookov a mobilných zariadení) s prístupovými právami používateľov a riadením identít.

10.3 P7S – Politika nástupu a ukončenia: zabezpečuje, aby vydávanie a spätné prevzatie aktív bolo súčasťou procesov životného cyklu pracovníkov.

10.4 P13S – Politika klasifikácie údajov a označovania: stanovuje pravidlá na určenie, či má byť aktívum klasifikované ako interné použitie alebo Dôverné.

10.5 P30S – Politika reakcie na incidenty: usmerňuje postupy reakcie, ak udalosť súvisiaca s aktívom vedie k narušeniu bezpečnosti alebo ochrany súkromia.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1: Vyžaduje prevádzkové opatrenia na správu aktív a ich ochranu počas používania.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.9: Podrobne upravuje identifikáciu aktív, priradenie vlastníctva, klasifikáciu a ich bezpečnú správu.

11.3 NIST SP 800-53 Rev

11.3.1 CM-8: Vyžaduje, aby organizácie vytvorili a udržiavali inventarizáciu systémových komponentov vrátane hardvéru, softvéru a virtuálnych aktív.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 30: Vyžaduje dokumentáciu spracovateľských činností, ktorá závisí od toho, či je známe, kde sú údaje uložené a na akých aktívach.

11.5 EÚ NIS

11.5.1 Článok 21(2)(a): Vyžaduje technické a organizačné opatrenia vrátane evidencie aktív na ochranu sietí a informačných systémov.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 5(8): Finančné subjekty musia v rámci riadenia rizík IKT viesť podrobnú inventarizáciu aktív IKT.

11.7 COBIT 2019

11.7.1 BAI09: Stanovuje, že IT aktíva sa musia spravovať počas celého životného cyklu – od obstarania po vyradenie – s jasne určeným vlastníctvom a kontrolami.