					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P12S					Název dokumentu: **Politika správy aktiv**							
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**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	Požadavky na správu aktiv
ISO/IEC 27002:2022	Opatření 5	Opatření pro správu aktiv
NIST SP 800-53 Rev. 5	CM-8	Evidence komponent systému
Směrnice EU NIS2	Článek 21 odst. 2 písm. a)	Evidence aktiv pro ochranu sítí a informačních systémů
Nařízení EU DORA	Článek 5 odst. 8	Požadavky na evidenci aktiv ICT
COBIT 2019	BAI	Řízení životního cyklu IT aktiv
Nařízení EU GDPR	Článek 30	Evidence činností zpracování osobních údajů

1. Účel

1.1 Tato politika stanoví, jak organizace identifikuje, eviduje, chrání a vyřazuje svá informační aktiva, včetně fyzických i digitálních součástí.

1.2 Cílem je snižovat provozní a bezpečnostní rizika zajištěním přehledu, odpovědnosti a bezpečného nakládání se všemi podnikovými aktivy v průběhu celého jejich životního cyklu.

1.3 Spolehlivá evidence aktiv podporuje soulad s právními předpisy, reakci na incidenty, plánování kontinuity činností a řízení rizik.

1.4 Tato politika rovněž podporuje certifikaci podle ISO/IEC 27001 a dokládá soulad s právními, finančními a kyberbezpečnostními povinnostmi podle rámců, jako jsou GDPR, směrnice NIS2 a nařízení DORA.

1.5 Pro malé a střední podniky (SME) je jednoduchý, avšak systematický přístup ke správě aktiv nezbytný, aby se předešlo nezaevidovaným a nespravovaným zařízením, ztrátě dat nebo neúspěchu při auditu, zejména při omezených personálních a technických kapacitách.

2. Rozsah

2.1 Tato politika se vztahuje na všechna aktiva vlastněná, pronajatá nebo jinak spravovaná organizací, včetně aktiv používaných v těchto oblastech:

2.1.1 kancelářská práce

2.1.2 práce na dálku nebo hybridní režim práce

2.1.3 terénní nebo mobilní činnosti

2.1.4 cloudová a externě zajišťovaná prostředí

2.2 Typy aktiv zahrnuté do rozsahu zahrnují mimo jiné:

2.2.1 Hardware: notebooky, stolní počítače, monitory, telefony, tablety, USB disky, routery, tiskárny, záložní média

2.2.2 Software: instalované aplikace, nástroje SaaS, operační systémy, antivirové nástroje, licence

2.2.3 Datová aktiva: úložiště podnikových dat, tabulkové soubory, zákaznické záznamy, zdrojový kód

2.2.4 Digitální přihlašovací údaje a služby: doménová jména, digitální certifikáty, API klíče, e-mailové účty, cloudové přístupy

2.2.5 Přístupová zařízení: klíče, čipové karty, přístupové přívěsky, biometrické tokeny

2.3 Do rozsahu této politiky spadají všichni zaměstnanci, smluvní pracovníci a poskytovatelé třetích stran, kteří nakládají s aktivy organizace.

2.4 Politika upravuje krátkodobá aktiva (např. notebooky pro konkrétní projekt), dlouhodobá aktiva i sdílená aktiva používaná více pracovníky.

3. Cíle

3.1 Zavést a udržovat úplnou a přesnou evidenci všech relevantních aktiv, průběžně aktualizovanou.

3.2 Zajistit, aby každé aktivum mělo určeného vlastníka odpovědného za jeho používání, uložení a vrácení.

3.3 Klasifikovat aktiva podle citlivosti, dopadu na obchodní činnost nebo regulatorní relevance tak, aby bylo možné uplatnit odpovídající úrovně ochrany.

3.4 Stanovit jasné postupy pro vydávání aktiv, jejich přeřazení, údržbu, hlášení ztrát a vyřazení.

3.5 Zajistit bezpečné nakládání s aktivy po celý jejich životní cyklus a zajistit, aby informace, které uchovávají, byly při likvidaci chráněny nebo bezpečně vymazány.

3.6 Snížit pravděpodobnost bezpečnostních incidentů způsobených neevidovanými, nevrácenými nebo nesprávně používanými aktivy organizace.

3.7 Podpořit soulad s relevantními právními předpisy (např. zásadou odpovědnosti podle GDPR) a normami pro certifikaci v oblasti kybernetické bezpečnosti.

4. Role a odpovědnosti

4.1 Generální ředitel (GM)

4.1.1 Je vlastníkem této politiky a odpovídá za zajištění implementace a dodržování postupů správy aktiv v celé organizaci.

4.1.2 Přezkoumává a schvaluje aktualizace evidence aktiv a v případě potřeby schvaluje vyřazení aktiv z provozu nebo jejich převod.

4.1.3 Musí být informován o každé významné ztrátě, odcizení nebo zneužití aktiv.

4.2 Vedoucí IT nebo určený správce aktiv

4.2.1 Udržuje evidenci aktiv (např. v tabulkovém souboru, ticketovacím systému nebo jednoduchém nástroji pro evidenci aktiv).

4.2.2 Přiřazuje vlastnictví aktiv a sleduje změny jejich stavu (např. nové, v používání, v opravě, vyřazené).

4.2.3 Ověřuje, že všechna vydaná aktiva jsou zdokumentována a přiřazena konkrétní osobě nebo organizační jednotce.

4.2.4 Zajišťuje, aby byly používány a dodržovány klasifikační štítky (např. Vnitřní použití, Důvěrné).

4.2.5 Koordinuje převzetí, sanitizaci a deaktivaci aktiv při ukončení používání nebo vyřazení.

4.2.6 Oznamuje všechny nevyřešené nesrovnalosti v evidenci aktiv generálnímu řediteli (GM).

[... 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 a dále vždy, když:

9.1.1 jsou zavedeny nové typy technologií nebo aktiv

9.1.2 se změní postupy evidence aktiv (např. zavedením nových nástrojů nebo platforem)

9.1.3 nové regulatorní požadavky ovlivní dohledatelnost nebo likvidaci aktiv

9.1.4 incident nebo audit odhalí mezeru ve stávajících postupech správy aktiv

9.2 Přezkumy musí probíhat za účasti generálního ředitele (GM) a vedoucího IT a musí zahrnovat aktualizace postupů nakládání s aktivy, šablon evidence a pokynů ke klasifikaci.

9.3 Všechny aktualizace musí být zdokumentovány a oznámeny dotčeným pracovníkům. Musí být veden a uchováván protokol změn v režimu správy verzí.

10. Související politiky a vazby

10.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Stanoví odpovědnost za vlastnictví politik a provoz IT.

10.2 P4S – Politika řízení přístupu: Propojuje používání aktiv (např. notebooků a mobilních zařízení) s přístupovými právy uživatelů a řízením identit a přístupů.

10.3 P7S – Politika nástupu a ukončení: Zajišťuje, aby vydávání a vracení aktiv byly součástí procesů životního cyklu pracovníků.

10.4 P13S – Politika klasifikace dat a označování: Poskytuje pravidla pro určení, zda má být aktivum klasifikováno jako Vnitřní použití nebo Důvěrné.

10.5 P30S – Politika reakce na incidenty: Upravuje postupy reakce, pokud událost související s aktivem vede k narušení bezpečnosti nebo ochrany soukromí.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1: Vyžaduje provozní opatření pro správu aktiv a jejich ochranu po celou dobu používání.

11.2 ISO/IEC 27002

11.2.1 Opatření 5.9: Stanoví, jak aktiva identifikovat, přiřadit jim vlastnictví, klasifikovat je a bezpečně spravovat.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-8: Vyžaduje, aby organizace vytvořily a udržovaly evidenci komponent systému, včetně hardwaru, softwaru a virtuálních aktiv.

11.4 Nařízení EU GDPR

11.4.1 Článek 30: Vyžaduje dokumentaci činností zpracování osobních údajů, která závisí na znalosti toho, kde jsou data uložena a na jakých aktivech.

11.5 Směrnice EU NIS2

11.5.1 Článek 21 odst. 2 písm. a): Požaduje technická a organizační opatření, včetně evidence aktiv, k ochraně sítí a informačních systémů.

11.6 Nařízení EU DORA

11.6.1 Článek 5 odst. 8: Finanční subjekty musí v rámci řízení ICT rizik udržovat podrobnou evidenci aktiv ICT.

11.7 COBIT 2019

11.7.1 BAI09: Stanoví, že IT aktiva musí být řízena po celý svůj životní cyklus — od pořízení po vyřazení — s jasně stanoveným vlastnictvím a opatřeními.