					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P12					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**

1. Účel

1.1 Tato politika stanoví závazné organizační požadavky na identifikaci, klasifikaci, správu a ochranu informačních aktiv v průběhu jejich životního cyklu. Podporuje celopodnikovou správu a řízení hardwarových, softwarových, datových, cloudových a nehmotných informačních aktiv, včetně mobilních, vzdálených a třetí stranou spravovaných prostředí.

1.2 Účelem této politiky je zajistit úplný přehled o prostředí informačních aktiv organizace, a tím umožnit účinná bezpečnostní opatření, jednoznačné přiřazení vlastnictví, zajištění souladu a odpovědné vyřazení z provozu nebo likvidaci.

1.3 Tato politika je v souladu s přílohou A.5.9 normy ISO/IEC 27001:2022, neboť stanoví povinnost vést centralizovanou evidenci informací a souvisejících aktiv. Zajišťuje odpovědnost tím, že každému aktivu přiřazuje vlastníka a uplatňuje ochranu řízenou klasifikací podle obchodní citlivosti a regulatorních požadavků.

2. Rozsah

2.1 Tato politika se vztahuje na všechny zaměstnance, smluvní pracovníky, dodavatele třetích stran a poskytovatele služeb, kteří spravují, používají, zpřístupňují, ukládají nebo zpracovávají informační aktiva vlastněná nebo kontrolovaná organizací.

2.2 Rozsah zahrnuje všechny kategorie aktiv, například:

2.2.1 Fyzická aktiva: notebooky, stolní počítače, mobilní zařízení, výměnná média, tiskárny, síťová zařízení

2.2.2 Digitální aktiva: software, aplikace, obrazy systémů, databáze, záložní data, šifrovací klíče

2.2.3 Informační aktiva: strukturovaná i nestrukturovaná data, zprávy, e-maily, duševní vlastnictví

2.2.4 Cloudová a virtuální aktiva: prostředí IaaS, SaaS a PaaS, virtuální stroje, kontejnery

2.2.5 Logická aktiva: doménová jména, licence, uživatelské účty, výchozí konfigurace

2.3 Tato politika se rovněž vztahuje na aktiva používaná při práci na dálku, v hybridním režimu nebo v rámci outsourcovaných služeb a zajišťuje jejich ochranu a přehled i v případě, že se fyzicky nenacházejí v prostorách organizace.

3. Cíle

3.1 Udržovat úplnou, přesnou a aktuální evidenci všech informačních aktiv organizace s definovanými atributy vlastnictví, klasifikace a umístění.

3.2 Přiřadit vlastníkům aktiv odpovědnost za klasifikaci, nakládání a ochranu aktiv pod jejich kontrolou v souladu s politikami správy dat a bezpečnosti.

3.3 Uplatňovat odpovídající klasifikaci a označování všech aktiv podle citlivosti, kritičnosti a regulatorních hledisek.

3.4 Chránit aktiva podle jejich klasifikace a související zbytkové expozice, včetně ukládání, přístupu, přenosu a likvidace.

3.5 Vynucovat postupy vracení aktiv a jejich bezpečné likvidace při ukončení pracovního poměru, ukončení smluvního vztahu nebo na konci životního cyklu aktiva.

3.6 Podporovat soulad s rámci, jako jsou ISO/IEC 27001, GDPR, NIS2, DORA a COBIT 2019, prostřednictvím strukturované správy aktiv a auditovatelnosti.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje Politiku správy aktiv a zajišťuje přidělení zdrojů pro její plnou implementaci.

4.1.2 Nese konečnou odpovědnost za ochranu a správu aktiv organizace v souladu s regulatorními a smluvními povinnostmi.

4.2 Ředitel informační bezpečnosti (CISO)

4.2.1 Je vlastníkem Politiky správy aktiv a zajišťuje její integraci do širšího systému řízení bezpečnosti informací (ISMS) organizace.

4.2.2 Přezkoumává výjimky a odchylky od této politiky a prosazuje strategie zmírňování rizik založené na posouzení rizik.

4.2.3 Dohlíží na pravidelné audity klasifikace aktiv, integrity evidence aktiv a souladu řízení životního cyklu aktiv.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumávána alespoň jednou ročně nebo v reakci na:

9.1.1 změny právních nebo regulatorních povinností, které mají dopad na klasifikaci aktiv nebo požadavky na evidenci,

9.1.2 zavedení nových kategorií aktiv nebo platforem pro jejich správu (např. cloud-native CMDB),

9.1.3 zjištění interního auditu nebo bezpečnostní incidenty související s nesprávnou správou aktiv,

9.1.4 organizační změny, které mají dopad na vlastnictví nebo kontroly životního cyklu.

9.2 Proces přezkumu zahajuje manažer IT aktiv a koordinuje jej s CISO, útvarem nákupu, právním oddělením a dotčenými vedoucími oddělení.

9.3 Mimořádné přezkumy mohou být spuštěny také v důsledku:

9.3.1 akvizice nebo odprodeje obchodních jednotek,

9.3.2 změn dodavatelů ovlivňujících aktiva spravovaná třetí stranou,

9.3.3 obnov technologií zahrnujících hromadné vyřazování z provozu nebo zřizování.

9.4 Všechny revize této politiky musí:

9.4.1 být vedeny v režimu správy verzí a uloženy v repozitáři dokumentace ISMS,

9.4.2 být schváleny vrcholovým vedením,

9.4.3 obsahovat shrnutí změn a jejich odůvodnění,

9.4.4 být sděleny všem dotčeným zainteresovaným stranám, včetně aktualizovaných postupů nebo školení k systémům, je-li to relevantní.

10. Související politiky a vazby

10.1 Tato politika funguje společně s následujícími souvisejícími politikami a podporuje jejich uplatňování:

10.1.1 P4 - Politika řízení přístupu: Zajišťuje, aby přehled o aktivech odpovídal přístupovým oprávněním a mechanismům řízení v systémech a datových prostředích.

10.1.2 P7 - Politika nástupu a ukončení: Upravuje včasné zřizování a vracení fyzických a logických aktiv při personálních změnách.

10.1.3 P13 - Politika klasifikace dat a označování: Stanoví závazná pravidla klasifikace aktiv, která určují označování, nakládání a postupy likvidace.

10.1.4 P14 - Politika uchovávání údajů a likvidace: Definuje lhůty a způsoby bezpečné likvidace digitálních a fyzických aktiv obsahujících informace.

10.1.5 P22 - Politika protokolování a monitorování: Umožňuje dohledatelnost přístupu k aktivům a jejich používání prostřednictvím systémového protokolování, viditelnosti koncových bodů a behaviorální analytiky.

10.1.6 P30 - Politika reakce na incidenty: Podporuje rychlou triáž, omezení dopadu a vyšetřování porušení souvisejících s aktivy, jako jsou ztracené notebooky nebo nesledovaná úložná média.

10.2 Tyto politiky tvoří ucelený rámec správy a řízení, který zajišťuje bezpečnou správu aktiv, přesnou evidenci a odpovídající nakládání v celém jejich životním cyklu.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s mezinárodně uznávanými normami informační bezpečnosti a regulatorními rámci, které vyžadují robustní správu aktiv v průběhu celého životního cyklu.

11.2 ISO/IEC 27001:

11.2.1 Článek 8.1 - Vyžaduje, aby organizace plánovaly, implementovaly a řídily procesy potřebné ke splnění požadavků informační bezpečnosti, včetně požadavků na správu životního cyklu aktiv.

11.3 ISO/IEC 27002:2022 - Opatření 5.9 až 5.11

11.3.1 Opatření 5.9 - Evidence informací a dalších souvisejících aktiv: Vyžaduje aktuální a úplnou evidenci všech aktiv relevantních pro zpracování informací.

11.3.2 Opatření 5.10 - Přípustné užívání informací a aktiv: Je podporováno pravidly používání, vlastnictvím a procesy vrácení.

11.3.3 Opatření 5.11 - Vrácení aktiv: Je implementováno prostřednictvím formálních postupů předání a vyřazení z provozu.

11.3.4 Tato opatření stanovují strukturované požadavky na identifikaci, označování, údržbu a sledování organizačních aktiv spolu s odpovídajícími odpovědnostmi vlastníků a správců po celý životní cyklus.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - Evidence komponent systému: Promítá se do centralizované správy aktiv, přehledu v reálném čase a vazby na provozní konfigurace.

11.4.2 RA-3 - Hodnocení rizik: Evidence aktiv slouží jako základní prvek pro modelování hrozeb a vyhodnocení rizik.

11.4.3 MP-6 - Sanitizace médií: Je vynucována prostřednictvím bezpečných metod likvidace definovaných v kontrolách životního cyklu aktiv a v politice likvidace dat.

11.5 GDPR (2016/679):

11.5.1 Článek 30 - Záznamy o činnostech zpracování: Vyžaduje, aby organizace dokumentovaly systémy, zařízení a repozitáře, které ukládají nebo zpracovávají osobní údaje.

11.5.2 Článek 32 - Zabezpečení zpracování: Je v souladu s vyhodnocením rizik na základě aktiv a s ochrannými opatřeními přizpůsobenými klasifikovaným aktivům a kritické infrastruktuře.

11.6 směrnice NIS2 (2022/2555):

11.6.1 Článek 21(2)(a, b): Ukládá přehled o aktivech a jejich evidenci jako základ pro analýzu rizik, ochranu a reakci na kybernetické bezpečnostní incidenty.

11.6.2 Článek 21(3): Potvrzuje nezbytnost strukturované správy aktiv jako součásti organizační bezpečnostní kultury.

11.7 nařízení DORA (2022/2554):

11.7.1 Článek 5 - Správa a řízení ICT a vnitřní kontrola: Vyžaduje, aby finanční subjekty řídily aktiva ICT s jasnými požadavky na evidenci, vlastnictví a ochranu.

11.7.2 Článek 9 - Rámec řízení rizik v oblasti ICT: Stanoví, že procesy správy aktiv musí podporovat zmírňování hrozeb, plánování kontinuity činností a odolnost služeb.

11.8 COBIT 2019:

11.8.1 BAI09 - Správa aktiv: Přímo odpovídá strukturované identifikaci, klasifikaci, používání a likvidaci podnikových aktiv.

11.8.2 DSS01 - Řízený provoz: Podporuje implementaci opatření, která zajišťují ochranu aktiv a průběžnou provozní správu a řízení.

11.8.3 MEA03 - Monitorování, hodnocení a posuzování souladu: Zajišťuje pravidelné audity opatření správy aktiv a jejich účinnosti ve vztahu k regulatornímu souladu.