					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P07S					Název dokumentu: **Politika nástupu a ukončení**							
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**

Soulad s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Články 6.2, 7	Požadavky na bezpečnost lidských zdrojů a bezpečnostní povědomí
ISO/IEC 27002:2022	Opatření 6.2, 6.5	Bezpečnostní postupy při nástupu a ukončení
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Ukončení pracovního poměru; životní cyklus účtů; plánování
směrnice NIS2	Článek 21(2)(h)	Bezpečnost lidských zdrojů a životní cyklus přístupových oprávnění
nařízení DORA	Článek 12	Řízení přístupu a revokace přístupů k ICT systémům
COBIT 2019	APO07, DSS01	Bezpečnost pracovníků, řízení logického a fyzického přístupu
GDPR	Článek 32	Zabezpečení osobních údajů v průběhu pracovněprávního vztahu

1. Účel

1.1 Tato politika stanoví proces nástupu nových zaměstnanců nebo smluvních pracovníků a bezpečného odebrání přístupu při odchodu osob nebo změně jejich role.

1.2 Zajišťuje, aby přístupová oprávnění byla zřizována pouze v rozsahu nezbytném podle zásady minimálních oprávnění, aby byla evidována všechna aktiva a aby byly bez prodlení provedeny kritické kroky, jako je deaktivace systémových přístupů a obnova dat.

1.3 Tato politika podporuje soulad, provozní integritu a ochranu dat prostřednictvím strukturovaných a auditovatelných činností při nástupu a ukončení.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny stálé i dočasné zaměstnance

2.1.2 smluvní pracovníky, konzultanty a stážisty

2.1.3 externí poskytovatele služeb se systémovým nebo fyzickým přístupem

2.2 Zahrnuje:

2.2.1 nástup: zřízení uživatelských účtů, přidělení přístupu, vydání vybavení

2.2.2 ukončení: odebrání přístupu, vrácení firemního majetku a bezpečné uzavření digitálních identit

2.2.3 interní změny rolí vyžadující změnu nastavení přístupu nebo přeřazení aktiv

2.3 Vztahuje se na všechna zařízení, platformy a lokality používané pro výkon pracovních činností.

3. Cíle

3.1 Zajistit, aby noví pracovníci obdrželi přístupová oprávnění a zdroje na základě ověřených rolí a odpovědností.

3.2 Potvrdit, že odcházejícím uživatelům budou nejpozději do konce jejich posledního pracovního dne zcela odebrána přístupová oprávnění do systémů i objektů.

3.3 Předcházet vzniku osiřelých účtů a nevrácených aktiv, která představují bezpečnostní riziko.

3.4 Vést dokumentované záznamy o činnostech souvisejících s nástupem, převody a ukončením.

3.5 Podporovat odpovědnost prostřednictvím kontrolních seznamů a koordinace rolí napříč útvary.

4. Role a odpovědnosti

4.1 generální ředitel

4.1.1 Schvaluje přístupová oprávnění pro role s vysokými oprávněními a vykonává dohled nad procesem nástupu a ukončení.

4.1.2 Zajišťuje, aby výjimky byly řádně odůvodněny a aby byla přijata nápravná opatření, pokud nejsou postupy dodržovány.

4.2 Office Manager / HR

4.2.1 Zahajuje proces nástupu nových pracovníků a informuje IT o odchodech.

4.2.2 Zajišťuje dokončení právní dokumentace (např. NDA) a potvrzení seznámení s bezpečnostními politikami.

4.2.3 Vede kontrolní seznamy pro nástup a ukončení a monitoruje dodržování této politiky.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 každoroční přezkum

9.1.1 Tato politika musí být přezkoumána nejméně jednou ročně generálním ředitelem a vedoucími HR a IT.

9.2 spouštěče dřívějšího přezkumu

9.2.1 Aktualizace musí proběhnout, pokud:

9.2.1.1 jsou zavedeny nové HR nebo IT systémy

9.2.1.2 dojde ke změně externího poskytovatele IT služeb nebo poskytované HR služby

9.2.1.3 bezpečnostní audity odhalí mezery v procesech

9.2.1.4 se změní regulatorní povinnosti (např. aktualizace GDPR)

9.2.1.5 dojde ke kritickému selhání při ukončení nebo k narušení bezpečnosti

9.3 řízení verzí a schvalování

9.3.1 Každá verze této politiky musí obsahovat:

9.3.1.1 číslo verze a datum

9.3.1.2 shrnutí změn

9.3.1.3 schválení generálním ředitelem

9.3.1.4 archivované předchozí verze uchovávané nejméně tři roky

9.4 komunikace a potvrzení seznámení

9.4.1 Veškerý personál odpovědný za nástup nebo ukončení musí být informován o všech aktualizacích této politiky. Každoroční školení bezpečnostního povědomí nebo opakovací instruktáže jsou povinné.

10. Související politiky a vazby

10.1 Tato politika podporuje následující dokumenty a je jimi podporována:

10.1.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: Zajišťuje odpovědnost v procesech přidělování přístupu a nástupu

10.1.2 P4S – Politika řízení přístupu: Stanoví technické vynucování zřizování přístupu podle rolí a deaktivace

10.1.3 P6S – Politika řízení rizik: Posuzuje rizika vyplývající ze selhání kontrol při nástupu a ukončení

10.1.4 P8S – Politika bezpečnostního povědomí a školení: Uplatňuje požadavky na seznámení pracovníků při nástupu

10.1.5 P30S – Politika reakce na incidenty (P30): Považuje neprovedené odebrání přístupových oprávnění nebo odcizení aktiv za bezpečnostní incidenty

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 6.2 – Stanoví požadavky na bezpečnost lidských zdrojů

11.1.2 Článek 7.2 – Ukládá školení bezpečnostního povědomí pro nové pracovníky

11.2 ISO/IEC 27002

11.2.1 Opatření 6.2 a 6.5 – Podrobně upravují bezpečnostní postupy při nástupu a ukončení pracovního poměru

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Postupy při ukončení pracovního poměru včetně deaktivace přístupu

11.3.2 AC-2 – Zajišťuje řízení životního cyklu účtů pro uživatelský přístup

11.3.3 PL-4 – Vyžaduje plánování personálních přechodů

11.4 GDPR

11.4.1 Článek 32 – Zajišťuje odpovídající bezpečnost během zaměstnání i po jeho ukončení, zejména při přístupu k osobním údajům

11.5 směrnice NIS2

11.5.1 Článek 21(2)(h) – Vyžaduje bezpečnost lidských zdrojů a kontroly životního cyklu přístupových oprávnění

11.6 nařízení DORA

11.6.1 Článek 12 – Vyžaduje, aby regulované finanční subjekty řídily přístup pracovníků k ICT systémům, včetně postupů revokace

11.7 COBIT 2019

11.7.1 APO07 – Řízení lidských zdrojů: stanoví požadavky na bezpečnost v průběhu životního cyklu pracovníků

11.7.2 DSS01 – Řízení provozu: zahrnuje řízení logického a fyzického přístupu při personálních přechodech