					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P07					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**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 7.2, Kapitola 6	Kompetence personálu, bezpečné začlenění a uplatňování odpovědností při ukončení nebo změně pracovního zařazení.
ISO/IEC 27002:2022	Opatření 6.2, 6.5, 5	Nástup, přístup a kontroly životního cyklu personálu.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Přesuny personálu a ukončení pracovního poměru, zásada minimálních oprávnění, auditní protokolování, řízení přístupu během změn personálu i po nich.
EU GDPR	Články 5(1)(f), 25, 32; bod odůvodnění 39	Omezení přístupu, důvěrnost, ochrana a přiměřená opatření pro osobní údaje zaměstnanců.
EU NIS2	Článek 21(2)(b, c, d)	Bezpečnostní opatření v oblasti personálu a provozu; zmírňování vnitřních hrozeb; procesy životního cyklu.
EU DORA	Články 5, 8, 9	Správa a řízení, interní ICT kontroly, ICT rizika, řízení incidentů při změnách personálu.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Lidské zdroje, řízení znalostí, bezpečnost a soulad při nástupu a ukončení.

1. Účel

1.1 Tato politika stanoví standardizované postupy pro řízení nástupu, interních převodů a ukončení u všech typů uživatelů.

1.2 Zajišťuje včasné a bezpečné zřízení přístupu a odebrání přístupových oprávnění k fyzickému i logickému přístupu a současně prosazuje důvěrnost, odpovědnost a vrácení aktiv.

1.3 Tato politika zmírňuje rizika spojená s neoprávněným přístupem, únikem dat a nevrácenými aktivy tím, že začleňuje kontroly nástupu a ukončení do procesů HR, IT a bezpečnosti.

1.4 Podporuje ISO/IEC 27001:2022, přílohu A, opatření 6.5 tím, že zajišťuje uplatňování bezpečnostních povinností personálu během pracovního nebo smluvního vztahu i po jeho skončení.

2. Rozsah

2.1 Tato politika se vztahuje na všechny zaměstnance, dodavatele, konzultanty, poskytovatele a další třetí strany, kterým byl udělen přístup k systémům, sítím, prostorám nebo datům organizace.

2.2 Upravuje celý životní cyklus:

2.2.1 nástupu (nástup do zaměstnání, uzavření smluvního vztahu nebo dočasné zapojení)

2.2.2 interních převodů nebo změn rolí

2.2.3 ukončení (výpověď, odchod do důchodu, ukončení pracovního poměru, vypršení smlouvy)

2.3 Politika pokrývá:

2.3.1 logický přístup (systémy, aplikace, cloudové služby, VPN)

2.3.2 fyzický přístup (průkazy, klíče, systémy vstupu do budov)

2.3.3 přidělená aktiva (notebooky, telefony, tokeny, přihlašovací údaje)

2.3.4 potvrzení seznámení s politikami a povinnosti zachování důvěrnosti

2.4 Všechna oddělení (HR, IT, správa budov a majetku, bezpečnost a vedení) odpovídají za plnění své role v procesech nástupu a ukončení.

3. Cíle

3.1 Zajistit, aby byl veškerému personálu udělen přístup pouze po splnění bezpečnostních, školicích a smluvních předpokladů.

3.2 Odebrat přístupová práva a vrátit organizační aktiva ihned při změně role nebo ukončení.

3.3 Zachovat důvěrnost, integritu a dostupnost organizačních aktiv během změn personálu.

3.4 Podpořit auditovatelnost a právní vymahatelnost prostřednictvím úplných záznamů o událostech nástupu a ukončení.

3.5 Snížit expozici vůči vnitřním hrozbám ověřováním a dokumentováním všech událostí přístupu souvisejících s personálem.

3.6 Uvést životní cyklus personálu organizace do souladu s bezpečnostními postupy založenými na rizicích a regulačními požadavky.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje tuto politiku a přiděluje pravomoci a zdroje pro procesy nástupu, ukončení a řízení přístupu.

4.1.2 Zajišťuje, aby změny personálu nevystavovaly organizaci nepřiměřenému bezpečnostnímu nebo právnímu riziku.

4.2 Lidské zdroje (HR)

4.2.1 Zahajují pracovní postupy nástupu a ukončení pro zaměstnance a oznamují příslušným oddělením změny.

4.2.2 Zajišťují, aby byly před udělením přístupu dokončeny prověrky spolehlivosti, smlouvy, dohody o mlčenlivosti a potvrzení seznámení s politikou.

4.2.3 Informují IT a správu budov a majetku o odchodech pracovníků v souladu se SLA pro oznamování.

4.2.4 Koordinují s právním oddělením a compliance uplatňování povinností po skončení pracovního poměru (např. doložek o mlčenlivosti).

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Frekvence přezkumu politiky

9.1.1 Tato politika musí být přezkoumána:

9.1.1.1 každoročně, nebo

9.1.1.2 po jakémkoli významném incidentu souvisejícím se zneužitím přístupu, ztrátou aktiv nebo selháním postupu

9.1.1.3 při implementaci významných změn platforem HR nebo IAM

9.1.1.4 při regulačních nebo právních změnách ovlivňujících osobní údaje nebo související povinnosti

9.2 Proces přezkumu a vlastnictví

9.2.1 Manažer ISMS a ředitel HR koordinují přezkum za účasti IT bezpečnosti, právního oddělení a compliance.

9.2.2 Všechny změny musí být schváleny vrcholovým vedením a Řídicím výborem ISMS pro bezpečnost informací.

9.2.3 Revidované verze musí být znovu distribuovány dotčeným oddělením a pracovníkům k opětovnému potvrzení seznámení.

9.3 Řízení dokumentu a uchovávání

9.3.1 Tato politika musí obsahovat:

9.3.2 řízení verzí, historii změn a datum účinnosti

9.3.3 odpovědného vlastníka a přezkoumávající osoby

9.3.4 klasifikaci politiky a záznam o schválení

9.3.5 Neplatné verze musí být archivovány po dobu minimálně 3 let v souladu s Politikou správy dokumentů.

10. Související politiky a vazby

10.1.1 Tato politika je přímo propojena s:

10.1.2 P1 – Politika informační bezpečnosti: Stanoví bezpečnostní cíle organizace, včetně správy a řízení přístupu personálu.

10.1.3 P4 – Politika řízení přístupu: Stanoví provozní požadavky na přidělování a odebírání systémového a fyzického přístupu na základě spouštěčů nástupu a ukončení.

10.1.4 P3 – Zásady přípustného užívání: Vyžadují potvrzení seznámení během nástupu a podporují uplatňování po ukončení.

10.1.5 P6 – Politika řízení rizik: Zajišťuje, že rizika přístupu uživatelů a změn jejich statusu jsou vyhodnocována a zmírňována v souladu se zásadami ISMS.

10.1.6 P11 – Politika řízení uživatelských účtů a oprávnění: Upravuje technická opatření pro zřizování přístupu a odebrání přístupových oprávnění na podporu této politiky.

10.2 Tyto politiky tvoří integrovaný systém opatření pro bezpečné a odpovědné řízení událostí v životním cyklu personálu.

11. Referenční normy a rámce

11.1 Tato politika je sladěna s mezinárodně uznávanými rámci pro bezpečnost, ochranu soukromí a správu a řízení IT, aby byly procesy nástupu a ukončení bezpečné, dohledatelné a v souladu s právními a organizačními požadavky.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 7.2 – Kompetence a Kapitola 6.2 – Cíle informační bezpečnosti: Tato politika podporuje zajištění kompetence personálu a bezpečné začlenění jednotlivců do rolí, v nichž ovlivňují cíle ISMS.

11.2.2 Příloha A Opatření 6.5 – Odpovědnosti po ukončení nebo změně zaměstnání: Tato politika plně uplatňuje opatření týkající se zbytkových přístupových práv, správy dat a smluvních povinností při odchodu.

11.2.3 Příloha A Opatření 5.9 – Prověřování a 6.2 – Podmínky zaměstnání: Postupy nástupu zahrnují ověřování minulosti a mechanismy potvrzení seznámení s politikou v souladu s těmito ustanoveními.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (ukončení pracovního poměru) a PS-5 (převedení zaměstnance): Tato politika zajišťuje strukturované odebrání nebo úpravu přístupových práv, fyzických průkazů a aktiv.

11.3.2 AC-2 (řízení účtů) a AC-6 (zásada minimálních oprávnění): Stanovené požadavky zajišťují, že přístup odpovídá roli a je bez prodlení odebrán, jakmile již není potřebný.

11.3.3 IA-4 (řízení identifikátorů) a IA-5 (řízení autentizačních prostředků): Podporuje bezpečnou správu přihlašovacích údajů během změn personálu i po nich.

11.3.4 CM-5 (omezení přístupu pro změny): Zabraňuje neoprávněným změnám po ukončení tím, že odnímá zvýšená přístupová práva.

11.3.5 AU-2 a AU-6: Protokolování a dohledatelnost přístupových událostí jsou posíleny prostřednictvím integrace IAM a auditní stopy.

11.4 GDPR / obecné nařízení o ochraně osobních údajů (2016/679):

11.4.1 Článek 5(1)(f): Chrání osobní údaje před neoprávněným přístupem, což je v této politice zajištěno odebráním uživatelského přístupu při ukončení.

11.4.2 Článek 32: Vyžaduje odpovídající technická a organizační opatření k zabezpečení osobních údajů během životního cyklu zaměstnání.

11.4.3 Článek 25 – ochrana osobních údajů již od návrhu: Zajišťuje, aby nástup a ukončení zahrnovaly minimalizaci dat, uchovávání a zákonné kontroly přístupu.

11.4.4 Bod odůvodnění 39: Zdůrazňuje omezení přístupu a důvěrnost, které tato politika svou strukturou podporuje.

11.5 Směrnice NIS2 (2022/2555):

11.5.1 Článek 21(2)(b, c, d): Vyžaduje bezpečnostní opatření v oblasti personálu a provozu k řešení řízení přístupu, zmírňování vnitřních hrozeb a procesů životního cyklu, které jsou v této politice promítnuty.

11.6 Nařízení DORA (2022/2554):

11.6.1 Článek 5 – správa a řízení a interní kontrola: Tato politika podporuje interní správu a řízení ICT související s lidským rizikem a řízením přístupu.

11.6.2 Článek 8 – řízení ICT rizik: Uplatňuje opatření na změny personálu, které by mohly vystavit kritická aktiva nebo regulovaná prostředí riziku.

11.6.3 Článek 9 – klasifikace a řízení incidentů: Zajišťuje, že porušení související s ukončením podléhají hlášení a jsou zmírňována prostřednictvím správného odebrání přístupových oprávnění a nakládání s aktivy.

11.7 COBIT 2019:

11.7.1 APO07 – Řízené lidské zdroje: Definuje role, odpovědnosti a činnosti životního cyklu pro nástup a ukončení v souladu s cíli správy a řízení.

11.7.2 BAI08 – Řízení znalostí: Posiluje dokumentování postupů, uchovávání znalostí a předání kontrol na konci pracovního poměru.

11.7.3 DSS05 – Řízené bezpečnostní služby: Uplatňuje deaktivaci uživatelů, kontrolu aktiv a odpovědnost během změn rolí.

11.7.4 MEA03 – Monitorování, hodnocení a posuzování souladu: Zajišťuje, že kontroly nástupu a ukončení jsou posuzovány v rámci interních i externích auditů.