					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P07					Názov dokumentu: **Politika nástupu a ukončenia pracovného vzťahu**							
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**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 7.2, Kapitola 6	Kompetencie pracovníkov, bezpečné začlenenie a uplatňovanie povinností pri ukončení alebo zmene pracovného vzťahu.
ISO/IEC 27002:2022	Kontroly 6.2, 6.5, 5	Kontroly procesu nástupu, prístupu a životného cyklu pracovníkov.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Prechod a ukončenie pracovného vzťahu pracovníkov, zásada minimálnych oprávnení, auditné logovanie, riadenie prístupu počas personálnych zmien a po nich.
GDPR EÚ	Články 5(1)(f), 25, 32; odôvodnenie 39	Obmedzenie prístupu, dôvernosť, ochrana a primerané kontroly pre personálne údaje.
NIS2 EÚ	Článok 21(2)(b, c, d)	Personálne a prevádzkové bezpečnostné opatrenia; zmierňovanie vnútorných hrozieb; procesy životného cyklu.
DORA EÚ	Články 5, 8, 9	Správa a riadenie, vnútorná kontrola IKT, riziká IKT, riadenie incidentov počas personálnych zmien.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Ľudské zdroje, riadenie znalostí, bezpečnosť a súlad pri nástupe a ukončení.

1. Účel

1.1 Táto politika stanovuje štandardizované postupy na riadenie procesu nástupu, interných presunov a ukončenia pracovného alebo zmluvného vzťahu pre všetky typy používateľov.

1.2 Zabezpečuje včasné a bezpečné zriaďovanie prístupov a odoberanie prístupových práv k fyzickému aj logickému prístupu a zároveň presadzuje dôvernosť, zodpovednosť a vrátenie aktív.

1.3 Táto politika zmierňuje riziká súvisiace s neoprávneným prístupom, únikom údajov a nevrátenými aktívami tým, že začleňuje kontroly nástupu a ukončenia do procesov HR, IT a bezpečnosti.

1.4 Podporuje kontrolu 6.5 prílohy A normy ISO/IEC 27001:2022 tým, že zabezpečuje uplatňovanie povinností personálnej bezpečnosti počas pracovného alebo zmluvného vzťahu aj po jeho skončení.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných pracovníkov, konzultantov, dodávateľov a ďalšie tretie strany, ktorým bol udelený prístup k systémom, sieťam, priestorom alebo údajom organizácie.

2.2 Upravuje celý životný cyklus:

2.2.1 nástup (prijatie do zamestnania, uzatvorenie zmluvného vzťahu alebo dočasné zapojenie)

2.2.2 interné presuny alebo zmeny roly

2.2.3 ukončenie (výpoveď, odchod do dôchodku, ukončenie pracovného pomeru, uplynutie zmluvy)

2.3 Politika pokrýva:

2.3.1 logický prístup (systémy, aplikácie, cloudové prostredia, VPN)

2.3.2 fyzický prístup (preukazy, kľúče, systémy vstupu do budovy)

2.3.3 pridelené aktíva (notebooky, telefóny, tokeny, prihlasovacie údaje)

2.3.4 potvrdenie oboznámenia sa s politikami a povinnosti zachovávať dôvernosť

2.4 Všetky útvary (HR, IT, správa zariadení, bezpečnosť a manažment) zodpovedajú za vykonávanie svojej úlohy v pracovných postupoch nástupu a ukončenia.

3. Ciele

3.1 Zabezpečiť, aby bol všetkým pracovníkom udelený prístup až po splnení bezpečnostných, školiacich a zmluvných predpokladov.

3.2 Zrušiť prístupové oprávnenia a získať späť aktíva organizácie bezodkladne pri zmene roly alebo ukončení.

3.3 Zachovať dôvernosť, integritu a dostupnosť aktív organizácie počas personálnych zmien.

3.4 Podporiť auditovateľnosť a právnu obhájiteľnosť prostredníctvom úplných záznamov o udalostiach nástupu a ukončenia.

3.5 Znížiť expozíciu voči vnútorným hrozbám validáciou a dokumentovaním všetkých udalostí prístupu súvisiacich s personálom.

3.6 Zosúladiť životný cyklus pracovníkov organizácie s bezpečnostnými postupmi založenými na riziku a regulačnými požiadavkami.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje túto politiku a prideľuje právomoci a zdroje pre procesy nástupu, ukončenia a riadenia prístupu.

4.1.2 Zabezpečuje, aby personálne zmeny nevystavovali organizáciu neprimeranému bezpečnostnému alebo právnemu riziku.

4.2 Ľudské zdroje (HR)

4.2.1 Iniciujú pracovné postupy nástupu a ukončenia pre zamestnancov a oznamujú relevantným útvarom zmeny.

4.2.2 Zabezpečujú, aby boli previerky spoľahlivosti, zmluvy, dohody o mlčanlivosti a potvrdenie oboznámenia sa s politikou dokončené pred udelením prístupu.

4.2.3 Informujú IT a správu zariadení o odchodoch pracovníkov v súlade s dohodnutými úrovňami služieb (SLA) pre notifikácie.

4.2.4 Koordinujú sa s právnym oddelením pri uplatňovaní povinností po skončení pracovného pomeru (napr. doložiek o mlčanlivosti).

[... 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 Frekvencia preskúmania politiky

9.1.1 Táto politika sa musí preskúmať:

9.1.1.1 každoročne, alebo

9.1.1.2 po každom podstatnom incidente zahŕňajúcom zneužitie prístupu, stratu aktív alebo zlyhanie postupu

9.1.1.3 pri zavedení významných zmien v platforme HR alebo IAM

9.1.1.4 pri regulačných alebo právnych zmenách, ktoré ovplyvňujú personálne údaje alebo povinnosti

9.2 Proces preskúmania a vlastníctvo

9.2.1 Manažér ISMS a riaditeľ HR koordinujú preskúmanie za účasti IT bezpečnosti, právneho oddelenia a funkcie súladu.

9.2.2 Všetky zmeny musí schváliť vrcholový manažment a Riadiaci výbor pre ISMS.

9.2.3 Revidované verzie musia byť opätovne distribuované dotknutým útvarom a pracovníkom na opätovné potvrdenie oboznámenia sa.

9.3 Riadenie dokumentu a uchovávanie

9.3.1 Táto politika musí obsahovať:

9.3.2 riadenie verzií, históriu zmien a dátum účinnosti

9.3.3 určeného vlastníka a preskúmavateľa(-ov)

9.3.4 klasifikáciu politiky a záznam o schválení

9.3.5 Neplatné verzie musia byť archivované minimálne 3 roky v súlade s Politikou správy dokumentov.

10. Súvisiace politiky a väzby

10.1.1 Táto politika je priamo prepojená s:

10.1.2 P1 – Politika informačnej bezpečnosti: stanovuje bezpečnostné ciele organizácie vrátane správy a riadenia prístupu pracovníkov.

10.1.3 P4 – Politika riadenia prístupu: stanovuje prevádzkové požiadavky na prideľovanie a zrušenie systémového a fyzického prístupu na základe spúšťačov nástupu a ukončenia.

10.1.4 P3 – Politika prijateľného používania: vyžaduje potvrdenie oboznámenia sa počas nástupu a podporuje uplatňovanie politiky po ukončení.

10.1.5 P6 – Politika riadenia rizík: zabezpečuje, aby riziká prístupu používateľov a personálnych zmien boli hodnotené a zmierňované v súlade so zásadami ISMS.

10.1.6 P11 – Politika správy používateľských účtov a oprávnení: upravuje technické kontrolné opatrenia pre zriaďovanie prístupu a odoberanie prístupových práv na podporu tejto politiky.

10.2 Tieto politiky tvoria integrovaný systém kontrol na bezpečné a preukázateľné riadenie udalostí životného cyklu pracovníkov.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými rámcami bezpečnosti, ochrany súkromia a správy a riadenia IT s cieľom zabezpečiť, aby procesy nástupu a ukončenia boli bezpečné, sledovateľné a v súlade s právnymi a organizačnými požiadavkami.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 7.2 – Kompetencie a Kapitola 6.2 – Ciele informačnej bezpečnosti: Táto politika podporuje vytváranie kompetencií pracovníkov a bezpečné začlenenie jednotlivcov do rolí, v ktorých ovplyvňujú ciele ISMS.

11.2.2 Príloha A, kontrola 6.5 – Povinnosti po ukončení alebo zmene pracovného pomeru: Táto politika v plnom rozsahu uplatňuje kontroly nad zostatkovými prístupovými právami, správou údajov a zmluvnými povinnosťami pri odchode.

11.2.3 Príloha A, kontrola 5.9 – preverovanie a 6.2 – podmienky zamestnania: Postupy nástupu zahŕňajú preverenie minulosti a mechanizmy potvrdenia oboznámenia sa s politikou v súlade s týmito ustanoveniami.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (ukončenie pracovného vzťahu) a PS-5 (pracovné preradenie): Táto politika presadzuje štruktúrované odobratie alebo úpravu prístupových práv, fyzických preukazov a aktív.

11.3.2 AC-2 (správa účtov) a AC-6 (zásada minimálnych oprávnení): Opatrenia zabezpečujú, aby bol prístup zosúladený s rolou a bezodkladne zrušený, keď už nie je potrebný.

11.3.3 IA-4 (správa identifikátorov) a IA-5 (správa autentifikátorov): Podporuje bezpečnú správu prihlasovacích údajov počas personálnych zmien a po nich.

11.3.4 CM-5 (obmedzenia prístupu pri zmenách): Predchádza neoprávneným zmenám po ukončení tým, že ruší zvýšené oprávnenia.

11.3.5 AU-2 a AU-6: Logovanie a sledovateľnosť udalostí prístupu sú posilnené integráciou IAM a auditnou stopou.

11.4 Nariadenie EÚ GDPR (2016/679):

11.4.1 Článok 5(1)(f): Chráni osobné údaje pred neoprávneným prístupom, čo sa v tejto politike zabezpečuje zrušením používateľského prístupu počas ukončenia.

11.4.2 Článok 32: Vyžaduje primerané technologické a organizačné kontrolné opatrenia na ochranu osobných údajov počas životného cyklu zamestnania.

11.4.3 Článok 25 – Ochrana údajov už od návrhu: Zabezpečuje, aby nástup a ukončenie zahŕňali minimalizáciu údajov, uchovávanie a zákonné kontroly prístupu.

11.4.4 Odôvodnenie 39: Zdôrazňuje obmedzenie prístupu a dôvernosť, ktoré sú podporené štruktúrou tejto politiky.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Článok 21(2)(b, c, d): Vyžaduje personálne a prevádzkové bezpečnostné opatrenia na riešenie riadenia prístupu, zmierňovania vnútorných hrozieb a procesov životného cyklu, čo sa odráža v tejto politike.

11.6 Nariadenie EÚ DORA (2022/2554):

11.6.1 Článok 5 – Správa a riadenie a vnútorná kontrola: Táto politika podporuje vnútornú správu a riadenie IKT vo vzťahu k ľudským rizikám a riadeniu prístupu.

11.6.2 Článok 8 – Riadenie rizík IKT: Uplatňuje kontroly pri personálnych zmenách, ktoré by mohli vystaviť kritické aktíva alebo regulované prostredia riziku.

11.6.3 Článok 9 – Klasifikácia a riadenie incidentov: Zabezpečuje, aby porušenia súvisiace s ukončením podliehali hláseniu a boli zmiernené prostredníctvom správneho zrušenia prístupov a nakladania s aktívami.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Definuje roly, zodpovednosti a činnosti životného cyklu pre nástup a ukončenie v súlade s cieľmi správy a riadenia.

11.7.2 BAI08 – Knowledge Management: Posilňuje dokumentovanie postupov, uchovávanie znalostí a odovzdanie kontrol pri skončení pracovného pomeru.

11.7.3 DSS05 – Managed Security Services: Presadzuje deaktiváciu používateľov, kontrolu aktív a zodpovednosť počas prechodov rolí.

11.7.4 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: Zabezpečuje, aby boli kontroly nástupu a ukončenia posudzované počas interných a externých auditov.