					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P07S					Názov dokumentu: **politika nástupu a ukončenia pracovného pomeru**							
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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 6.2, 7	Požiadavky na bezpečnosť ľudských zdrojov a bezpečnostné povedomie
ISO/IEC 27002:2022	Kontroly 6.2, 6.5	Bezpečnostné postupy pri nástupe a ukončení pracovného pomeru
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Ukončenie pracovného pomeru; životný cyklus účtov; plánovanie
EÚ NIS2	Článok 21(2)(h)	Bezpečnosť ľudských zdrojov a životný cyklus prístupových oprávnení
EÚ DORA	Článok 12	Riadenie prístupu a odoberanie prístupových oprávnení k systémom IKT
COBIT 2019	APO07, DSS01	Bezpečnosť zamestnancov, logický a fyzický prístup
EÚ GDPR	Článok 32	Bezpečnosť osobných údajov počas trvania pracovnoprávneho vzťahu

1. Účel

1.1 Táto politika stanovuje proces nástupu nových zamestnancov alebo zmluvných pracovníkov a bezpečného odoberania prístupových práv pri odchode osôb alebo pri zmene ich roly.

1.2 Zabezpečuje, aby sa prístup prideľoval v rozsahu zodpovedajúcom zásade minimálnych oprávnení, aby boli všetky aktíva evidované a aby sa kritické kroky, ako deaktivácia systémov a obnova údajov, vykonali bezodkladne.

1.3 Táto politika podporuje súlad, prevádzkovú integritu a ochranu údajov prostredníctvom štruktúrovaných a auditovateľných činností pri nástupe a ukončení pracovného pomeru.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých stálych a dočasných zamestnancov,

2.1.2 zmluvných pracovníkov, konzultantov a stážistov,

2.1.3 externých poskytovateľov služieb so systémovým alebo fyzickým prístupom.

2.2 Zahŕňa:

2.2.1 proces nástupu: vytváranie používateľských účtov, prideľovanie prístupu, vydávanie vybavenia,

2.2.2 ukončenie pracovného pomeru: odoberanie prístupových práv, vrátenie podnikových aktív a bezpečné ukončenie digitálnych identít,

2.2.3 interné zmeny roly vyžadujúce úpravu prístupových oprávnení alebo opätovné pridelenie aktív.

2.3 Vzťahuje sa na všetky zariadenia, platformy a miesta používané na výkon pracovných činností.

3. Ciele

3.1 Zabezpečiť, aby noví pracovníci dostali prístup a zdroje na základe overených rolí a zodpovedností.

3.2 Potvrdiť, že odchádzajúcim používateľom budú do konca ich posledného pracovného dňa úplne odobraté prístupy do systémov a priestorov.

3.3 Predchádzať osirelým účtom a nevráteným aktívam, ktoré predstavujú bezpečnostné riziko.

3.4 Udržiavať zdokumentované záznamy o nástupe, zmenách pracovného zaradenia a ukončení pracovného pomeru.

3.5 Podporovať zodpovednosť prostredníctvom kontrolných zoznamov a koordinácie rolí medzi útvarmi.

4. Roly a zodpovednosti

4.1 Generálny manažér

4.1.1 Schvaľuje prístup pre privilegované roly a vykonáva dohľad nad procesom nástupu a ukončenia pracovného pomeru.

4.1.2 Zabezpečuje, aby boli výnimky riadne odôvodnené a aby sa prijali nápravné opatrenia, ak sa procesy nedodržiavajú.

4.2 Office manažér / HR

4.2.1 Iniciuje proces nástupu nových pracovníkov a informuje IT o odchodoch.

4.2.2 Zabezpečuje dokončenie právnych dokumentov (napr. dohody o mlčanlivosti) a potvrdení o oboznámení sa s bezpečnostnými politikami.

4.2.3 Udržiava kontrolné zoznamy pre nástup a ukončenie pracovného pomeru a monitoruje dodržiavanie tejto politiky.

[... 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 Ročné preskúmanie

9.1.1 Túto politiku musí najmenej raz ročne preskúmať generálny manažér a vedúci HR/IT.

9.2 Spúšťače skoršieho preskúmania

9.2.1 Aktualizácia sa musí vykonať, ak:

9.2.1.1 sa zavedú nové systémy HR alebo IT,

9.2.1.2 dôjde k zmene externého poskytovateľa IT služieb alebo poskytovateľa spravovaných HR služieb,

9.2.1.3 bezpečnostné audity odhalia nedostatky v procesoch,

9.2.1.4 sa zmenia regulačné povinnosti (napr. aktualizácie GDPR),

9.2.1.5 dôjde ku kritickému zlyhaniu procesu ukončenia alebo k bezpečnostnému incidentu.

9.3 Riadenie verzií a schvaľovanie

9.3.1 Každá verzia tejto politiky musí obsahovať:

9.3.1.1 číslo verzie a dátum,

9.3.1.2 súhrn zmien,

9.3.1.3 schválenie generálnym manažérom,

9.3.1.4 archivované predchádzajúce verzie uchovávané najmenej tri roky.

9.4 Komunikácia a potvrdenie oboznámenia sa

9.4.1 Všetci pracovníci zodpovední za nástup alebo ukončenie musia byť informovaní o každej aktualizácii politiky. Ročné školenie bezpečnostného povedomia alebo opakované poučenie sú povinné.

10. Súvisiace politiky a prepojenia

10.1 Táto politika podporuje tieto politiky a zároveň je nimi podporovaná:

10.1.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: zabezpečuje zodpovednosť v procesoch prístupu a nástupu,

10.1.2 P4S – Politika riadenia prístupu: stanovuje technické uplatňovanie prideľovania prístupu na základe rolí a deaktivácie,

10.1.3 P6S – Politika riadenia rizík: posudzuje riziká vyplývajúce zo zlyhaní kontrol pri nástupe a ukončení,

10.1.4 P8S – Politika bezpečnostného povedomia a školení: stanovuje požiadavky na vstupné poučenie pracovníkov počas nástupu,

10.1.5 P30S – Politika reakcie na incidenty: považuje zlyhanie odoberania prístupov alebo krádež aktív za bezpečnostné incidenty.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.2 – stanovuje požiadavky na bezpečnosť ľudských zdrojov.

11.1.2 Kapitola 7.2 – stanovuje povinnosť školenia bezpečnostného povedomia pre nových pracovníkov.

11.2 ISO/IEC 27002

11.2.1 Kontroly 6.2 a 6.5 – podrobne upravujú bezpečnostné postupy pri nástupe a ukončení pracovného pomeru.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – postupy pri ukončení pracovného pomeru vrátane deaktivácie prístupu.

11.3.2 AC-2 – zabezpečuje riadenie životného cyklu účtov pre prístup používateľov.

11.3.3 PL-4 – vyžaduje plánovanie personálnych zmien.

11.4 EÚ GDPR

11.4.1 Článok 32 – vyžaduje primeranú úroveň bezpečnosti počas zamestnania aj po jeho skončení, najmä pri prístupe k osobným údajom.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(h) – vyžaduje kontroly bezpečnosti ľudských zdrojov a životného cyklu prístupových oprávnení.

11.6 EÚ DORA

11.6.1 Článok 12 – vyžaduje, aby regulované finančné subjekty riadili prístup zamestnancov k systémom IKT vrátane postupov odoberania prístupových oprávnení.

11.7 COBIT 2019

11.7.1 APO07 – Riadenie ľudských zdrojov: stanovuje požiadavky na bezpečnosť v rámci životného cyklu zamestnancov.

11.7.2 DSS01 – Riadenie prevádzky: zahŕňa riadenie logického a fyzického prístupu počas personálnych zmien.