					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P04S					Názov dokumentu: **Politika riadenia prístupu**							
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**

Súvisiace normy a predpisy

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 5	
ISO/IEC 27002:2022	Kontroly: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 až AC-5	
Nariadenie EÚ GDPR	Článok 32	
Smernica EÚ NIS2	Článok 21(2)(b)	
Nariadenie EÚ DORA	Článok 9	
COBIT 2019	APO07, DSS01	

1. Účel

1.1. Táto politika stanovuje, ako organizácia riadi prístup k systémom, údajom a priestorom s cieľom zabezpečiť, aby k informáciám mali prístup iba oprávnené osoby na základe pracovnej potreby.

1.2. Stanovuje jasné pravidlá pre zriaďovanie prístupu, zmeny, monitorovanie a odoberanie prístupových práv s cieľom minimalizovať riziko neoprávneného prístupu a podporiť súlad s uplatniteľnými právnymi predpismi a normami.

1.3. Táto politika uplatňuje zásadu minimálnych oprávnení a vyžaduje, aby bol prístup obmedzený na nevyhnutné minimum potrebné na výkon pracovných úloh.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky osoby, ktoré používajú alebo spravujú prístup k IT systémom, sieťam, údajom alebo priestorom organizácie, vrátane:

2.1.1. zamestnancov

2.1.2. zmluvných pracovníkov

2.1.3. dočasných pracovníkov

2.1.4. externých poskytovateľov IT služieb

2.2. Politika sa vzťahuje na prístup k:

2.2.1. podnikovým aplikáciám, zdieľaným súborovým úložiskám a databázam

2.2.2. systémom elektronickej pošty, VPN a systémom vzdialeného prístupu

2.2.3. cloudovým službám používaným na pracovné účely

2.2.4. fyzickému prístupu do zabezpečených priestorov, ako sú kancelárie alebo serverovne

2.3. Táto politika je záväzná pre všetky zariadenia (podnikové alebo schválené v režime používania vlastných zariadení (BYOD)), platformy a lokality.

3. Ciele

3.1. Zabezpečiť, aby sa prístupové práva udeľovali len na základe formálneho schválenia, podľa roly a pracovného odôvodnenia.

3.2. Predchádzať neoprávnenému alebo neprimerane rozsiahlemu prístupu k citlivým údajom, systémom alebo infraštruktúre.

3.3. Stanoviť jasné postupy pre zriaďovanie prístupu, zmeny a ukončenie používateľského prístupu.

3.4. Vyžadovať pravidelné preskúmania prístupových práv a automatizované alebo manuálne zaznamenávanie auditných záznamov na podporu auditov.

3.5. Podporiť technické presadzovanie obmedzení prístupu prostredníctvom riadenia konfigurácie a monitorovania.

4. Roly a zodpovednosti

4.1. Generálny riaditeľ (GM)

4.1.1. Schvaľuje túto politiku a zabezpečuje dostupnosť zdrojov na zavedenie účinného riadenia prístupu.

4.1.2. Schvaľuje výnimky a preskúmava ročné audity prístupov.

4.2. IT manažér / externý poskytovateľ IT služieb

4.2.1. Zabezpečuje zriaďovanie prístupov, zmeny a rušenie používateľských účtov.

4.2.2. Vedie register riadenia prístupu so všetkými aktivitami (vytvorenie, zmena, odobratie).

4.2.3. Zavádza riadenie prístupu na základe rolí (RBAC) a uplatňuje silnú autentifikáciu (napr. viacfaktorovú autentifikáciu (MFA)).

4.2.4. Kontroluje záznamy o prístupe z hľadiska podozrivej aktivity a zistené skutočnosti oznamuje generálnemu riaditeľovi (GM).

[... 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 politiky

9.1.1. IT manažér musí túto politiku preskúmať každoročne. Každá zmena v právnom, technickom alebo organizačnom kontexte musí viesť k jej bezodkladnej aktualizácii.

9.2. Spúšťače preskúmania

9.2.1. Politika sa musí preskúmať aj vtedy, ak nastane niektorá z nasledujúcich skutočností:

9.2.2. významné zmeny systémov alebo migrácie do cloudového prostredia

9.2.3. zmeny rolí alebo organizačnej štruktúry

9.2.4. bezpečnostný incident zahŕňajúci neoprávnený prístup

9.2.5. regulačné zmeny (napr. aktualizácie GDPR, NIS2 alebo DORA)

9.3. Dokumentovanie a komunikovanie zmien

9.3.1. Revízie musia byť zaznamenané s históriou verzií, schválením generálnym riaditeľom (GM) a oznámené všetkým dotknutým osobám.

9.4. Dostupnosť a školenie

9.4.1. Táto politika musí byť sprístupnená všetkým zamestnancom a príslušné školenie sa musí poskytovať v rámci procesu nástupu a následne každý rok.

10. Súvisiace politiky a väzby

10.1. Táto politika sa musí uplatňovať v koordinácii s nasledujúcimi SME politikami, aby sa zabezpečilo úplné uplatňovanie bezpečných postupov riadenia prístupu:

10.1.1. P3S – Politika prijateľného používania: zabezpečuje, aby používatelia rozumeli prijateľnému správaniu pri používaní prideleného prístupu.

10.1.2. P5S – Politika riadenia zmien: zabezpečuje, aby prístupové práva boli v súlade so schválenými zmenami systémov.

10.1.3. P7S – Politika nástupu a ukončenia: vymedzuje spúšťacie body pre zriaďovanie prístupu a rušenie používateľských prístupov.

10.1.4. P17S – Politika ochrany údajov a súkromia: zabezpečuje, aby riadenie prístupu bolo v súlade s ochranou osobných údajov.

10.1.5. P30S – Politika reakcie na incidenty: vymedzuje, ako sa riadia a vyšetrujú incidenty súvisiace s prístupom (napr. zneužitie alebo porušenia).

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.15 – Vyžaduje formalizované politiky a procesy riadenia prístupu.

11.2. ISO/IEC 27002

11.2.1. Kontroly 5.15 – 5.17 – Stanovujú podrobné usmernenia pre prístup založený na rolách, riadenie životného cyklu používateľov a správu privilegovaného prístupu.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 až AC-5 – Vyžadujú štruktúrované politiky riadenia prístupu vrátane autorizácie účtov, preskúmania a monitorovania.

11.4. Nariadenie EÚ GDPR

11.4.1. Článok 32 – Vyžaduje technické a organizačné opatrenia (ako je riadenie prístupu) na zabezpečenie bezpečnosti a dôvernosti údajov.

11.5. Smernica EÚ NIS2

11.5.1. Článok 21(2)(b) – Ukladá požiadavku na prevádzkové riadenie prístupu a systémy riadenia identít s cieľom zabrániť neoprávnenému prístupu do systémov.

11.6. Nariadenie EÚ DORA

11.6.1. Článok 9 – Zdôrazňuje bezpečné riadenie rizík IKT vrátane robustného riadenia prístupu pre finančné subjekty.

11.7. COBIT 2019

11.7.1. APO07 – Riadená bezpečnosť: vyžaduje vymedzené a uplatňované zodpovednosti za prístup.

11.7.2. DSS01 – Riadenie prevádzky: zahŕňa postupy na riadenie logického prístupu a udržiavanie bezpečného prevádzkového prostredia.