					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P04S					Název dokumentu: **Politika řízení přístupu**							
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	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 5	
ISO/IEC 27002:2022	Opatření 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 až AC-5	
GDPR EU	Článek 32	
EU NIS2	Článek 21 odst. 2 písm. b)	
EU DORA	Článek 9	
COBIT 2019	APO07, DSS01	

1. Účel

1.1. Tato politika stanoví, jak organizace řídí přístup k systémům, datům a prostorám tak, aby k informacím měly přístup pouze oprávněné osoby na základě obchodní potřeby.

1.2. Stanoví jasná pravidla pro zřizování přístupu, jeho změny, monitorování a odebírání s cílem minimalizovat riziko neoprávněného přístupu a podpořit soulad s příslušnými právními předpisy a normami.

1.3. Tato politika uplatňuje zásadu nejmenších oprávnění a vyžaduje, aby byl přístup omezen na nezbytné minimum potřebné k výkonu pracovních činností.

2. Rozsah

2.1. Tato politika se vztahuje na všechny osoby, které používají nebo spravují přístup k IT systémům, sítím, datům nebo prostorám organizace, včetně:

2.1.1. zaměstnanců

2.1.2. smluvních pracovníků

2.1.3. dočasných pracovníků

2.1.4. externích poskytovatelů IT služeb

2.2. Zahrnuje přístup k:

2.2.1. firemním aplikacím, síťovým sdílením a databázím

2.2.2. e-mailu, VPN a systémům vzdáleného přístupu

2.2.3. cloudovým službám používaným pro obchodní účely

2.2.4. fyzickému přístupu do zabezpečených prostor, jako jsou kanceláře nebo serverovny

2.3. Tato politika je závazná pro všechna zařízení (firemní nebo schválená v režimu používání soukromých zařízení (BYOD)), platformy a lokality.

3. Cíle

3.1. Zajistit, aby byla přístupová práva udělována pouze po formálním schválení na základě role a obchodního odůvodnění.

3.2. Předcházet neoprávněnému nebo nadměrnému přístupu k citlivým datům, systémům nebo infrastruktuře.

3.3. Vymezit jasné postupy pro zřizování přístupových práv, jejich změny a ukončení uživatelského přístupu.

3.4. Vyžadovat pravidelné revize přístupových práv a automatizované nebo manuální protokolování na podporu auditů.

3.5. Podpořit technické vynucování omezení přístupu prostřednictvím konfigurace a monitorování.

4. Role a odpovědnosti

4.1. Generální ředitel

4.1.1. Schvaluje tuto politiku a zajišťuje dostupnost zdrojů pro zavedení účinných opatření řízení přístupu.

4.1.2. Schvaluje výjimky a přezkoumává každoroční audity přístupu.

4.2. IT manažer / externí poskytovatel IT služeb

4.2.1. Zajišťuje zřizování přístupu, změny a rušení uživatelských účtů.

4.2.2. Vede registr řízení přístupu obsahující veškeré činnosti (zřízení, změny, odebrání).

4.2.3. Zavádí řízení přístupu na základě rolí (RBAC) a uplatňuje silnou autentizaci (např. vícefaktorovou autentizaci (MFA)).

4.2.4. Přezkoumává záznamy o přístupu z hlediska podezřelé aktivity a hlásí zjištěné problémy generálnímu řediteli.

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

9. Požadavky na přezkum a aktualizaci

9.1. Každoroční přezkum politiky

9.1.1. IT manažer musí tuto politiku každoročně přezkoumat. Jakékoli změny v právním, technickém nebo organizačním kontextu musí vést k okamžité aktualizaci.

9.2. Spouštěče přezkumu

9.2.1. Politika musí být přezkoumána také v případě, že nastane některá z následujících skutečností:

9.2.2. významné změny systémů nebo migrace do cloudu

9.2.3. změny rolí nebo organizační struktury

9.2.4. bezpečnostní incident zahrnující neoprávněný přístup

9.2.5. změny právních předpisů (např. aktualizace GDPR, NIS2 nebo DORA)

9.3. Dokumentování a komunikace změn

9.3.1. Změny musí být zaznamenány včetně historie verzí, schválení generálním ředitelem a musí být komunikovány všem dotčeným osobám.

9.4. Dostupnost a školení

9.4.1. Tato politika musí být zpřístupněna všem pracovníkům a příslušné školení musí být poskytováno v rámci onboardingu a následně každoročně.

10. Související politiky a vazby

10.1. Tato politika se uplatňuje ve spojení s následujícími SME politikami, aby bylo zajištěno úplné prosazování bezpečných postupů řízení přístupu:

10.1.1. P3S – Zásady přípustného užívání: zajišťují, aby uživatelé rozuměli přípustnému chování v rámci uděleného přístupu.

10.1.2. P5S – Politika řízení změn: zajišťuje, aby přístupová práva byla v souladu se schválenými změnami systémů.

10.1.3. P7S – Politika nástupu a ukončení: vymezuje spouštěcí body pro zřizování přístupových práv a odebrání přístupových oprávnění uživatelů.

10.1.4. P17S – Politika ochrany údajů a soukromí: zajišťuje, aby opatření řízení přístupu byla v souladu s ochranou osobních údajů.

10.1.5. P30S – Politika reakce na incidenty: vymezuje, jak jsou řízeny a vyšetřovány incidenty související s přístupem (např. zneužití nebo narušení bezpečnosti).

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.15 – Vyžaduje formalizované politiky a procesy řízení přístupu.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.15–5.17 – Stanoví podrobné pokyny pro přístup na základě rolí, řízení životního cyklu uživatelů a správu privilegovaného přístupu.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 až AC-5 – Vyžadují strukturované politiky pro řízení přístupu, včetně autorizace účtů, přezkumu a monitorování.

11.4. GDPR EU

11.4.1. Článek 32 – Vyžaduje technická a organizační opatření (např. řízení přístupu) k zajištění bezpečnosti a důvěrnosti dat.

11.5. Směrnice EU NIS2

11.5.1. Článek 21 odst. 2 písm. b) – Ukládá zavedení provozního řízení přístupu a systémů řízení identit s cílem předcházet neoprávněnému přístupu do systémů.

11.6. EU DORA

11.6.1. Článek 9 – Zdůrazňuje bezpečné řízení ICT rizik, včetně robustního řízení přístupu pro finanční subjekty.

11.7. COBIT 2019

11.7.1. APO07 – Řízená bezpečnost: vyžaduje definované a uplatňované odpovědnosti za přístup.

11.7.2. DSS01 – Řízení provozu: zahrnuje postupy pro správu logického přístupu a udržování bezpečného provozního prostředí.