					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P04					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**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitoly 5.15, 5.17, 5.18	Řízení logického a fyzického přístupu
ISO/IEC 27002:2022	Opatření 8.2, 8.3	Řízení přístupu na základě rolí a řízení identit
NIST SP 800-53 Rev. 5	AC-1 až AC-20, IA-1 až IA-8	Kontroly účtů a přístupu, identita a autentizace
GDPR EU	Články 5 odst. 1 písm. f), 32 odst. 1 písm. b); bod odůvodnění 39	Ochrana osobních údajů a minimalizace přístupu
směrnice EU NIS2	Článek 21 odst. 2 písm. c–e)	Řízení přístupu, autentizace uživatelů a ochrana aktiv
nařízení EU DORA	Články 6, 9 odst. 2	Přístup uživatelů a IKT, silné kontroly a třetí strany
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Nástup, provoz, monitorování, soulad

1. Účel

1.1 Tato politika stanoví závazné zásady, odpovědnosti a požadavky na kontrolní opatření pro řízení přístupu k informačním systémům, aplikacím, fyzickým prostorám a datovým aktivům v celé organizaci.

1.2 Zajišťuje, aby byl přístup udělován na základě obchodní potřeby, pracovní role a postoje k riziku, a uplatňuje zásadu minimálních oprávnění, princip potřeby znát a oddělení povinností.

1.3 Tato politika podporuje implementaci kapitoly 5.15 normy ISO/IEC 27001:2022 a souvisejících opatření upravujících logický a fyzický přístup, autentizaci uživatelů a řízení životního cyklu přístupu.

1.4 Tato politika tvoří základ ochrany digitálních a fyzických zdrojů před neoprávněným použitím, zneužitím nebo narušením.

2. Rozsah

2.1 Tato politika se vztahuje na všechny uživatele, systémy a prostory v rozsahu ISMS, včetně:

2.1.1 zaměstnanců, smluvních pracovníků, dodavatelů a dočasných pracovníků,

2.1.2 lokální infrastruktury, systémů hostovaných v cloudu a hybridních prostředí,

2.1.3 veškerého firemního majetku – hardwaru, softwaru, dat a zabezpečených fyzických prostor,

2.1.4 logického přístupu (např. systémy, sítě, aplikace, API) a fyzického přístupu (např. budovy, datová centra).

2.2 Upravuje přístup v celém životním cyklu identity a interakce se zdroji, od nástupu a zřizování přístupu po změny rolí a ukončení.

2.3 Politika se dále vztahuje na používání soukromých zařízení (BYOD) a vzdálený přístup a zajišťuje, aby bezpečnostní opatření byla konzistentní napříč lokalitami a modely vlastnictví zařízení.

3. Cíle

3.1 Zavést bezpečné řízení přístupu na základě rolí, které podporuje provozní integritu a soulad s právními předpisy.

3.2 Zajistit, aby přístupová práva byla řádně schvalována, monitorována a včas odebírána.

3.3 Předcházet neoprávněnému přístupu, eskalaci oprávnění a přetrvávání neaktuálních přístupových práv.

3.4 Podporovat principy Zero Trust tak, že přístup je ve výchozím nastavení odepřen, pokud není výslovně schválen a odůvodněn.

3.5 Poskytovat auditorům a zainteresovaným stranám ujištění prostřednictvím přezkumů přístupu založených na důkazech, prováděných automatizovaně, a prostřednictvím uplatňování této politiky.

3.6 Začlenit řízení přístupu do obchodních procesů, událostí životního cyklu v HR a technických architektur.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Schvaluje politiku řízení přístupu a zajišťuje odpovídající rozpočet a personální kapacity pro její uplatňování.

4.1.2 Přezkoumává rizika řízení přístupu v rámci přezkoumání vedením a přiděluje odpovědnost na strategické úrovni.

4.2 Ředitel informační bezpečnosti (CISO) / manažer ISMS

4.2.1 Odpovídá za rámec řízení přístupu a zajišťuje jeho soulad s ISO/IEC 27001 a souvisejícími normami.

4.2.2 Koordinuje uplatňování politiky, testování kontrol, nápravná opatření a vykazování metrik řízení přístupu.

4.2.3 Dohlíží na modelování přístupu založené na rizicích a monitoruje nedostatky v systémových kontrolách.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Spouštěče přezkumu a četnost

9.1.1 Tato politika musí být přezkoumána:

9.1.1.1 každoročně, nebo

9.1.1.2 po zásadní změně IT infrastruktury, regulatorních požadavků nebo postoje k riziku,

9.1.1.3 po incidentech, které odhalí slabiny v řízení přístupu,

9.1.1.4 při významných změnách v technologiích autentizace nebo platformách identit.

9.2 Pravomoc a proces přezkumu

9.2.1 CISO nebo určený vedoucí ISMS řídí cyklus přezkumu a zahrnuje do něj:

9.2.1.1 zjištění interního auditu,

9.2.1.2 výsledky a metriky přezkumů přístupu,

9.2.1.3 právní a regulatorní aktualizace,

9.2.1.4 změny technologických platforem.

9.2.2 Všechny změny musí být schváleny vrcholovým vedením a oznámeny všem zainteresovaným stranám.

9.2.3 Dotčení uživatelé mohou být při významných aktualizacích vyzváni k opětovnému potvrzení seznámení s politikou.

9.3 Řízení verzí a dokumentace

9.3.1 Hlavní verze musí být uložena v repozitáři dokumentace ISMS s následujícími metadaty:

9.3.1.1 číslo verze a protokol změn,

9.3.1.2 datum účinnosti a datum příštího přezkumu,

9.3.1.3 vlastník a schvalující orgán,

9.3.1.4 distribuční záznamy a záznamy o potvrzení seznámení.

9.3.2 Nahrazené verze musí být archivovány a dostupné po dobu nejméně 3 let.

10. Související politiky a vazby

10.1 Tato politika je funkčně závislá na následujících politikách a musí být vykládána společně s nimi:

10.1.1 P01 – Politika informační bezpečnosti: definuje závazek organizace v oblasti bezpečnosti a očekávání na vysoké úrovni v oblasti řízení přístupu.

10.1.2 P03 – Zásady přípustného užívání: stanoví pravidla chování pro přístup a odpovědnost uživatelů za řádné používání systémů.

10.1.3 P05 – Politika řízení změn: upravuje, jak musí být změny konfigurací přístupu, rolí nebo skupinových struktur bezpečně implementovány a testovány.

10.1.4 P07 – Politika nástupu a ukončení: upravuje přidělování a odebírání přístupových práv v souladu s událostmi životního cyklu uživatele.

10.1.5 P11 – Politika správy uživatelských účtů a oprávnění: zavádí kontroly na úrovni účtů a doplňuje tuto politiku o pokyny pro technické vynucování přístupu.

10.2 Tyto politiky společně poskytují soudržný a vymahatelný rámec správy přístupu napříč organizačními jednotkami a technologiemi.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:2022:

11.1.1 Kapitola 5.15 – Řízení přístupu: Tato politika naplňuje požadavek na řízení přístupu k informacím a dalším souvisejícím aktivům na základě obchodních požadavků a požadavků informační bezpečnosti.

11.1.2 Kapitola 5.17 – Řízení identit a kapitola 5.18 – Autentizační informace: Tyto požadavky jsou zavedeny prostřednictvím zřizování identit, mechanismů autentizace a přiřazování oprávnění.

11.1.3 Opatření přílohy A 8.2 (Řízení přístupu) a 8.3 (Řízení identit): Poskytují základ pro cíle opatření této politiky, včetně přístupu na základě rolí, integrace životního cyklu uživatele a ochrany privilegovaného přístupu.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 Rodina AC (AC-1 až AC-20): Tato politika podporuje požadavky NIST na řízení přístupu pro fyzické i logické systémy, včetně definování politiky (AC-1), správy účtů (AC-2) a oddělení povinností (AC-5).

11.2.2 Rodina IA (IA-1 až IA-8): Poskytuje vodítka pro autentizaci identity, ochranu přihlašovacích údajů a MFA.

11.2.3 AU-2, AU-12: Požadavky na protokolování a audit uplatňované touto politikou podporují odpovědnost uživatelů a vyšetřování incidentů.

11.2.4 PE-2 až PE-6: Zabývají se omezeními fyzického přístupu, která tato politika částečně uplatňuje prostřednictvím kontrol průkazů a oprávnění vstupu do budov.

11.3 GDPR (2016/679):

11.3.1 Článek 5 odst. 1 písm. f): Osobní údaje musí být chráněny před neoprávněným přístupem. Tato politika zajišťuje technické a procesní uplatňování tohoto principu.

11.3.2 Článek 32 odst. 1 písm. b): Vyžaduje zavedení řízení přístupu, pseudonymizace a šifrování k zabránění neoprávněnému zpracování osobních údajů.

11.3.3 Bod odůvodnění 39: Vyžaduje minimalizaci přístupu k osobním údajům, která je zde prosazována prostřednictvím zásady minimálních oprávnění a požadavků na odůvodnění přístupu.

11.4 Směrnice NIS2 (2022/2555):

11.4.1 Článek 21 odst. 2 písm. c–e): Tato politika umožňuje technická a organizační opatření pro řízení přístupu, autentizaci uživatelů a ochranu aktiv u základních i významných subjektů.

11.5 Nařízení DORA (2022/2554):

11.5.1 Článek 6: Vyžaduje politiky řízení rizik IKT, které výslovně zahrnují řízení přístupu uživatelů a kontroly životního cyklu identity. Tato politika tento požadavek naplňuje pro finanční sektor a sektor služeb IKT.

11.5.2 Článek 9 odst. 2: Tato politika podporuje uplatňování silných kontrol přístupu jako součásti řízení služeb IKT třetích stran a služeb v rámci skupiny.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: Prosazuje kontroly nástupu a ukončení na podporu správy přístupu.

11.6.2 BAI03 – Managed Solutions Identification and Build: Začleňuje požadavky na řízení přístupu do návrhu systémů a procesů změn.

11.6.3 DSS01 – Managed Operations a DSS05 – Managed Security Services: Upravují uplatňování omezení logického přístupu a monitorování porušení.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Podporuje auditní a zajišťovací mechanismy pro ověřování účinnosti řízení přístupu.