					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P04					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 5.15, 5.17, 5.18	riadenie logického a fyzického prístupu
ISO/IEC 27002:2022	Kontroly 8.2, 8.3	prístup na základe rolí a riadenie identít
NIST SP 800-53 Rev. 5	AC-1 až AC-20, IA-1 až IA-8	riadenie účtov a prístupu, identifikácia a autentifikácia
Nariadenie EÚ GDPR	Články 5 ods. 1 písm. f), 32 ods. 1 písm. b); odôvodnenie 39	ochrana údajov a minimalizácia
Smernica EÚ NIS2	Článok 21 ods. 2 písm. c) až e)	riadenie prístupu, autentifikácia používateľov a ochrana aktív
Nariadenie EÚ DORA	Články 6, 9 ods. 2	prístup používateľov k IKT, silné kontroly, tretie strany
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	nástup, prevádzka, monitorovanie, súlad

1. Účel

1.1 Táto politika stanovuje záväzné zásady, zodpovednosti a požiadavky na kontroly riadenia prístupu k informačným systémom, aplikáciám, fyzickým priestorom a dátovým aktívam v celej organizácii.

1.2 Zabezpečuje, aby bol prístup udeľovaný na základe pracovnej potreby, pracovnej roly a rizikového profilu, pričom sa uplatňujú zásada minimálnych oprávnení, zásada potreby vedieť a oddelenie povinností.

1.3 Táto politika podporuje implementáciu kapitoly 5.15 normy ISO/IEC 27001:2022 a súvisiacich kontrol upravujúcich logický a fyzický prístup, autentifikáciu používateľov a riadenie životného cyklu prístupu.

1.4 Táto politika tvorí základ ochrany digitálnych a fyzických aktív pred neoprávneným použitím, zneužitím alebo kompromitáciou.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých používateľov, systémy a priestory v rozsahu ISMS vrátane:

2.1.1 zamestnancov, zmluvných pracovníkov, dodávateľov a dočasného personálu

2.1.2 infraštruktúry v interných priestoroch, systémov prevádzkovaných v cloudovom prostredí a hybridných prostredí

2.1.3 všetkých podnikových aktív – hardvéru, softvéru, údajov a chránených fyzických priestorov

2.1.4 logického prístupu (napr. systémy, siete, aplikácie, API) a fyzického prístupu (napr. budovy, dátové centrá)

2.2 Upravuje prístup počas celého životného cyklu identity a interakcie so zdrojmi, od nástupu a zriadenia prístupu až po zmenu roly a ukončenie prístupu.

2.3 Politika sa vzťahuje aj na používanie vlastných zariadení (BYOD) a scenáre vzdialeného prístupu s cieľom zabezpečiť konzistentné kontroly naprieč lokalitami a modelmi vlastníctva zariadení.

3. Ciele

3.1 Zaviesť bezpečné riadenie prístupu na základe rolí, ktoré podporuje prevádzkovú integritu a súlad s požiadavkami.

3.2 Zabezpečiť, aby boli prístupové práva primerane schvaľované, monitorované a včas odoberané.

3.3 Predchádzať neoprávnenému prístupu, eskalácii oprávnení a pretrvávaniu neaktuálnych prístupových práv.

3.4 Podporovať princípy Zero Trust tým, že prístup sa štandardne zamieta, ak nie je výslovne schválený a odôvodnený.

3.5 Poskytovať uistenie audítorom a zainteresovaným stranám prostredníctvom automatizovaných revízií prístupových práv založených na dôkazoch a uplatňovania tejto politiky.

3.6 Začleniť riadenie prístupu do podnikových procesov, udalostí životného cyklu ľudských zdrojov a technických architektúr.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje politiku riadenia prístupu a zabezpečuje primeraný rozpočet a personálne kapacity na jej uplatňovanie.

4.1.2 Preskúmava riziká riadenia prístupu v rámci preskúmania manažmentom a prideľuje zodpovednosť na strategickej úrovni.

4.2 CISO / manažér ISMS

4.2.1 Zodpovedá za rámec riadenia prístupu a zabezpečuje jeho súlad s normou ISO/IEC 27001 a súvisiacimi normami.

4.2.2 Koordinuje uplatňovanie politiky, testovanie kontrol, nápravné opatrenia a vykazovanie metrík riadenia prístupu.

4.2.3 Dohliada na modelovanie prístupu na základe rizík a monitoruje systémové nedostatky v kontrolách.

[... 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 Spúšťače a frekvencia preskúmania

9.1.1 Táto politika musí byť preskúmaná:

9.1.1.1 každoročne alebo

9.1.1.2 po významnej zmene IT infraštruktúry, regulačných požiadaviek alebo rizikového profilu

9.1.1.3 po incidentoch, ktoré odhalia slabiny v riadení prístupu

9.1.1.4 pri významných zmenách v autentifikačných technológiách alebo platformách identít

9.2 Právomoc a proces preskúmania

9.2.1 CISO alebo určený vedúci ISMS riadi cyklus preskúmania, pričom zohľadňuje:

9.2.1.1 auditné zistenia vnútorného auditu

9.2.1.2 výsledky a metriky revízie prístupových práv

9.2.1.3 právne a regulačné aktualizácie

9.2.1.4 zmeny technologických platforiem

9.2.2 Všetky revízie musia byť schválené vrcholovým manažmentom a oznámené všetkým zainteresovaným stranám.

9.2.3 Dotknutí používatelia môžu byť pri podstatných aktualizáciách požiadaní o opätovné potvrdenie oboznámenia sa s politikou.

9.3 Riadenie verzií a dokumentácia

9.3.1 Hlavná verzia sa musí uchovávať v repozitári dokumentácie ISMS s týmito metadátami:

9.3.1.1 číslo verzie a zoznam zmien

9.3.1.2 dátum účinnosti a dátum nasledujúceho preskúmania

9.3.1.3 vlastník a schvaľujúci orgán

9.3.1.4 distribúcia a záznamy o potvrdení oboznámenia sa

9.3.2 Nahradené verzie musia byť archivované a dostupné minimálne 3 roky.

10. Súvisiace politiky a väzby

10.1 Táto politika je funkčne závislá od nižšie uvedených politík a musí sa vykladať spolu s nimi:

10.1.1 P01 – Politika informačnej bezpečnosti: Definuje záväzok organizácie v oblasti bezpečnosti a očakávania na vysokej úrovni pre riadenie prístupu.

10.1.2 P03 – Politika prijateľného používania: Stanovuje pravidlá správania pri prístupe a zodpovednosť používateľov za konanie pri riadnom používaní systémov.

10.1.3 P05 – Politika riadenia zmien: Upravuje, ako sa musia bezpečne implementovať a testovať zmeny konfigurácie prístupu, rolí alebo skupinových štruktúr.

10.1.4 P07 – Politika nástupu a ukončenia: Riadi zriaďovanie a odoberanie prístupových práv v súlade s udalosťami životného cyklu používateľa.

10.1.5 P11 – Politika správy používateľských účtov a oprávnení: Prevádza kontroly na úrovni účtov do prevádzky a dopĺňa túto politiku o technické pravidlá uplatňovania prístupu.

10.2 Tieto politiky spoločne poskytujú ucelený a vynútiteľný rámec správy a riadenia prístupov naprieč organizačnými jednotkami a technológiami.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:2022

11.1.1 Kapitola 5.15 – Riadenie prístupu: Táto politika plní požiadavku na riadenie prístupu k informáciám a ďalším súvisiacim aktívam na základe podnikových požiadaviek a požiadaviek informačnej bezpečnosti.

11.1.2 Kapitola 5.17 – Riadenie identít a kapitola 5.18 – Autentifikačné informácie: Tieto požiadavky sa realizujú prostredníctvom zriaďovania identít, mechanizmov autentifikácie a prideľovania oprávnení.

11.1.3 Kontroly prílohy A 8.2 (Politika riadenia prístupu) a 8.3 (Riadenie identít): Poskytujú základ pre ciele kontrol tejto politiky vrátane prístupu na základe rolí, integrácie životného cyklu používateľa a ochrany privilegovaného prístupu.

11.2 NIST SP 800-53 Rev. 5

11.2.1 Rodina AC (AC-1 až AC-20): Táto politika podporuje požiadavky NIST na riadenie prístupu pre fyzické aj logické systémy vrátane definície politiky (AC-1), riadenia účtov (AC-2) a oddelenia povinností (AC-5).

11.2.2 Rodina IA (IA-1 až IA-8): Poskytuje usmernenia pre autentifikáciu identity, ochranu prihlasovacích údajov a MFA.

11.2.3 AU-2, AU-12: Požiadavky na logovanie a audit uplatňované podľa tejto politiky podporujú zodpovednosť používateľov a vyšetrovanie incidentov.

11.2.4 PE-2 až PE-6: Riešia obmedzenia fyzického prístupu, ktoré táto politika čiastočne uplatňuje prostredníctvom riadenia preukazov a oprávnení vstupu do budov.

11.3 Nariadenie EÚ GDPR (2016/679)

11.3.1 Článok 5 ods. 1 písm. f): Osobné údaje musia byť chránené pred neoprávneným prístupom. Táto politika zabezpečuje technické a procesné uplatňovanie tejto zásady.

11.3.2 Článok 32 ods. 1 písm. b): Vyžaduje implementáciu riadenia prístupu, pseudonymizácie a šifrovania na predchádzanie neoprávnenému spracúvaniu osobných údajov.

11.3.3 Odôvodnenie 39: Vyžaduje minimalizáciu prístupu k osobným údajom, ktorá sa tu uplatňuje prostredníctvom zásady minimálnych oprávnení a požiadaviek na odôvodnenie prístupu.

11.4 Smernica EÚ NIS2 (2022/2555)

11.4.1 Článok 21 ods. 2 písm. c) až e): Táto politika umožňuje technické a organizačné opatrenia pre riadenie prístupu, autentifikáciu používateľov a ochranu aktív v rámci základných a dôležitých subjektov.

11.5 Nariadenie EÚ DORA (2022/2554)

11.5.1 Článok 6: Vyžaduje politiky riadenia rizík IKT, ktoré výslovne zahŕňajú riadenie prístupu používateľov a kontroly životného cyklu identít. Táto politika túto požiadavku spĺňa pre finančný sektor a sektor služieb IKT.

11.5.2 Článok 9 ods. 2: Táto politika podporuje uplatňovanie silných kontrol prístupu ako súčasti riadenia služieb IKT tretích strán a vnútroskupinových služieb.

11.6 COBIT 2019

11.6.1 APO07 – Managed Human Resources: Uplatňuje kontroly nástupu a ukončenia spolupráce na podporu správy a riadenia prístupov.

11.6.2 BAI03 – Managed Solutions Identification and Build: Začleňuje požiadavky na riadenie prístupu do návrhu systémov a procesov riadenia zmien.

11.6.3 DSS01 – Managed Operations a DSS05 – Managed Security Services: Upravujú uplatňovanie obmedzení logického prístupu a monitorovanie porušení.

11.6.4 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: Podporuje auditné a uisťovacie mechanizmy na overovanie účinnosti riadenia prístupu.