					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P11					Název dokumentu: **Politika správy uživatelských účtů a oprávnění**							
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	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Článek 6.1.3, článek 8	-
ISO/IEC 27002:2022	Opatření 5.15-5	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
GDPR	Články 5(1)(f), 32; bod odůvodnění 39	-
směrnice NIS2	Články 21(2)(a, d), 21(3)	-
nařízení DORA	Články 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Účel

1 Tato politika stanoví povinná opatření pro správu uživatelských účtů a oprávnění ve všech informačních systémech a službách. Zajišťuje, aby byl přístup ke zdrojům organizace udělován na základě ověřené identity, potřeby vyplývající z pracovní role a zásad minimálních oprávnění a oddělení povinností.

1.1 Podporuje závazek organizace k bezpečnosti informací zavedením strukturovaných a auditovatelných procesů pro zřizování účtů, přidělování oprávnění, monitorování používání a rušení účtů.

1.2 Tato politika je zásadní pro snižování rizika neoprávněného přístupu, zneužití oprávnění, vnitřních hrozeb a nesouladu s příslušnými regulačními rámci.

2. Rozsah

2.1 Tato politika se vztahuje na všechny zaměstnance a smluvní pracovníky, poskytovatele služeb třetích stran, konzultanty a další osoby, kterým byl udělen přístup k IT zdrojům, aplikacím nebo datům organizace.

2.2 Upravuje všechny systémy a prostředí, v nichž jsou uplatňovány mechanismy autentizace uživatelů a řízení přístupu, včetně mimo jiné:

2.2.1 podnikových aplikací a databází

2.2.2 cloudových platforem a prostředí SaaS

2.2.3 operačních systémů a administrátorských konzolí

2.2.4 nástrojů vzdáleného přístupu a VPN

2.2.5 systémů pro správu identit a přístupů (IAM)

2.3 Politika se vztahuje na standardní i privilegované uživatelské účty a zahrnuje opatření pro:

2.3.1 vytváření, změny a deaktivaci účtů

2.3.2 eskalaci oprávnění a delegování

2.3.3 řízení relací a monitorování

2.3.4 metody autentizace a správu přihlašovacích údajů

3. Cíle

3.1 Zajistit, aby všechny uživatelské účty byly jednoznačně identifikovatelné, řádně schválené a přidělované pouze po formálním ověření potřeby.

3.2 Uplatňovat zásadu minimálních oprávnění a předcházet zbytečnému nebo nadměrnému přístupu prostřednictvím přísných opatření pro přidělování a používání privilegovaných účtů.

3.3 Vyžadovat včasnou aktualizaci stavu účtů na základě změn pracovního zařazení nebo role, včetně okamžité deaktivace při ukončení pracovního poměru nebo spolupráce.

3.4 Umožnit proaktivní odhalování a nápravu neaktivních, zneužívaných nebo neoprávněných účtů prostřednictvím protokolování, přezkumů a automatizace.

3.5 Zachovat soulad s ISO/IEC 27001:2022 a souvisejícími normami a plnit povinnosti podle relevantních právních a regulačních rámců, jako jsou GDPR, směrnice NIS2, nařízení DORA a COBIT 2019.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její uplatňování v celé organizaci.

4.1.2 Přezkoumává a schvaluje všechny formální výjimky nebo případy nouzového přístupu.

4.1.3 Informuje vrcholové vedení o auditních zjištěních souvisejících s účty a eskaluje rizika.

4.2 manažer správy přístupů / IT administrátor

4.2.1 Udržuje a provozuje technická opatření pro správu životního cyklu uživatelských účtů.

4.2.2 Provádí zřizování přístupů, odebírání přístupových oprávnění a správu oprávnění na základě schválené žádosti.

4.2.3 Vede autoritativní registr všech uživatelských účtů, jejich stavu a úrovně oprávnění.

4.2.4 Podporuje audity a přezkumy souladu poskytováním logů a zpráv o činnosti.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumávána nejméně jednou ročně nebo při významných změnách v:

9.1.1 organizační struktuře nebo podnikových procesech

9.1.2 IT systémech, platformách identit nebo metodách přístupu

9.1.3 regulačních nebo smluvních požadavcích souvisejících s řízením identit a přístupů

9.2 ředitel informační bezpečnosti (CISO) společně s manažerem správy přístupů odpovídá za zahájení procesu přezkumu a koordinaci zpětné vazby od zainteresovaných stran.

9.3 Mimořádné přezkumy mohou být vyvolány:

9.3.1 bezpečnostními incidenty souvisejícími se zneužitím účtů

9.3.2 auditními zjištěními poukazujícími na nedostatky ve správě životního cyklu účtů

9.3.3 nasazením nových nástrojů pro správu identit nebo správu privilegovaných přístupů (PAM)

9.4 Aktualizace této politiky musí být:

9.4.1 vedeny v režimu správy verzí a zaznamenány v repozitáři dokumentace ISMS

9.4.2 komunikovány všem relevantním zainteresovaným stranám, včetně vedoucích oddělení, IT provozu a HR

9.4.3 podpořeny aktualizovanými školicími materiály a procesními příručkami

9.5 Všechny změny musí být schváleny vrcholovým vedením nebo Řídicím výborem pro bezpečnost informací a zaznamenány pro účely auditu.

10. Související politiky a vazby

10.1 Tato politika je provozně propojena s následujícími souvisejícími politikami v rámci ISMS a je jimi podporována:

10.1.1 P4 Politika řízení přístupu: Stanoví zastřešující zásady a mechanismy řízení přístupu, včetně opatření založených na pravidlech a rolích.

10.1.2 P7 Politika nástupu a ukončení: Poskytuje procesní kroky pro zahájení a ukončení uživatelského přístupu v návaznosti na kroky HR.

10.1.3 P8 Politika povědomí o bezpečnosti informací a školení: Posiluje odpovědnosti uživatelů za bezpečnost účtů a ochranu přihlašovacích údajů.

10.1.4 P13 Politika klasifikace a označování dat: Určuje úrovně přístupu podle klasifikace dat a zajišťuje, aby hranice oprávnění odpovídaly úrovním citlivosti.

10.1.5 P22 Politika protokolování a monitorování: Zajišťuje, že auditní stopa je shromažďována pro všechny činnosti související s účty a je přezkoumávána za účelem odhalení anomálií nebo neoprávněného použití.

10.1.6 P30 Politika reakce na incidenty: Upravuje eskalaci, zamezení šíření a činnosti po incidentu v případech zneužití oprávnění nebo neoprávněné činnosti účtů.

10.2 Každá z těchto politik působí ve vzájemné součinnosti za účelem uplatňování uceleného rámce řízení identit a přístupů založeného na rizicích napříč organizací.

11. Referenční normy a rámce

11.1 Tato politika je v souladu s celosvětově uznávanými normami kybernetické bezpečnosti a regulačními rámci, které vyžadují bezpečnou správu identit, přístupů a oprávnění jako základní součást bezpečnosti informací organizace.

11.2 ISO/IEC 27001:

11.2.1 Článek 6.1.3 vyžaduje, aby organizace určily, vyhodnotily a ošetřily rizika bezpečnosti informací, čímž činí správu přístupů a oprávnění formálním opatřením založeným na rizicích začleněným do procesu plánování ISMS.

11.2.2 Článek 8.1 – Provozní plánování a řízení: Posiluje zavedení technických a procesních ochranných opatření, která upravují uživatelský a privilegovaný přístup.

11.3 ISO/IEC 27002:2022 – Opatření 5.15 až 5:

11.3.1 Opatření 5.15 – řízení přístupu uživatelů: Podporuje formální procesy pro zřizování přístupu, schvalování přístupu a pravidelný přezkum přístupových práv.

11.3.2 Opatření 5.16 – správa identit: Zavádí jednoznačnost identity, opatření životního cyklu a vynucování bezpečné autentizace.

11.3.3 Opatření 5.17 zajišťuje, že přidělování a používání privilegovaných přístupových práv je přísně řízeno, dohledatelné a v souladu se zásadou minimálních oprávnění v celém životním cyklu uživatelského účtu.

11.3.4 Opatření 5.18 – privilegovaná přístupová práva: Je plně pokryto prostřednictvím přidělování oprávnění podle rolí, auditu a požadavků na schvalování zvýšeného přístupu.

11.4 Tato opatření usměrňují strukturovanou implementaci registrace účtů, rušení registrace, oddělení oprávnění a používání autentizačních informací. Politika prosazuje správu životního cyklu identity, just-in-time přístup a monitorování zvýšených relací s cílem zabránit neoprávněnému používání systému.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Politika řízení přístupu) a AC-2 (Správa účtů): Mapováno prostřednictvím požadavků politiky na schvalování přístupů, mapování rolí a audit uživatelských účtů.

11.5.2 AC-5 (Oddělení povinností) a AC-6 (zásada minimálních oprávnění): Naplněno prostřednictvím omezení oprávnění, souladu s pracovní rolí a dvojího schválení pro vysoce rizikové úkoly.

11.5.3 IA-2 až IA-5 (Identifikace a autentizace): Vynucováno prostřednictvím silných mechanismů autentizace, pravidel životního cyklu přihlašovacích údajů a požadavků na MFA.

11.5.4 AU-2, AU-12 (auditní protokolování a analýza): Řešeno prostřednictvím zaznamenávání relací a monitorování privilegovaných činností v citlivých prostředích.

11.6 GDPR (2016/679):

11.6.1 Článek 32 – Zabezpečení zpracování: Vyžaduje opatření řízení přístupu a mechanismy ověření identity k ochraně osobních údajů. Je naplněn požadavkem na schvalování účtů, přezkumy oprávnění a silná autentizační opatření.

11.6.2 Článek 5(1)(f) – Integrita a důvěrnost: Zajišťuje, aby k osobním údajům přistupovali pouze oprávnění uživatelé s legitimními rolemi, což je posíleno uplatňováním správy účtů.

11.6.3 Bod odůvodnění 39: Požaduje jasné omezení přístupu a odpovědnost; tato politika podporuje plnou dohledatelnost uživatelských identit a přidělení oprávnění.

11.7 směrnice NIS2 (2022/2555):

11.7.1 Článek 21(2)(a, d): Vyžaduje, aby subjekty uplatňovaly politiky správy přístupu a bezpečné nakládání s přihlašovacími údaji a privilegovanými relacemi, což je podporováno opatřeními této politiky pro zřizování přístupu, monitorování a správu výjimek.

11.7.2 Článek 21(3): Podporuje disciplínu přístupu a silné zajištění identity v kritických odvětvích, což je naplněno používáním jedinečných identifikátorů, RBAC a časově omezeného zvýšeného přístupu.

11.8 nařízení DORA (2022/2554):

11.8.1 Článek 5 – správa a řízení ICT a kontroly: Nařizuje formalizované procesy pro správu uživatelů ICT, které jsou pokryty dokumentovaným zřizováním přístupu, deaktivací a ošetřením výjimek.

11.8.2 Článek 9 – Řízení rizik v oblasti ICT: Ukládá organizacím zabezpečit systémy prostřednictvím omezení přístupu a monitorování, což je řešeno pomocí MFA, protokolování privilegovaného přístupu a centralizovaných přezkumů.

11.9 COBIT 2019:

11.9.1 DSS01 – Řízený provoz: Podporuje uplatňování standardizovaných provozních opatření, včetně správy životního cyklu uživatelských účtů a dokumentace přístupů.

11.9.2 DSS05 – Řízené bezpečnostní služby: Odráží bezpečnou správu uživatelských a systémových oprávnění a podporuje zmírňování rizik prostřednictvím zásady minimálních oprávnění a ověření auditní stopy.

11.9.3 APO13 – Řízená bezpečnost: Vyžaduje správu přístupu napříč digitálními aktivy, což je naplněno formalizovanými postupy schvalování účtů a rolí s požadavky na pravidelný přezkum.