					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P11S					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	Články 5.3, 8	Role, odpovědnosti a provozní plánování/řízení pro správu přístupu uživatelů
ISO/IEC 27002:2022	Opatření 8	Opatření pro přidělování, přezkum a odebírání zvýšených oprávnění
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Zřizování účtů, monitorování, zásada minimálních oprávnění a oddělení povinností
EU NIS2	Článek 21(2)(d)	správa přístupu uživatelů pro základní a důležité subjekty
EU DORA	Článek 9(2)(b)	správa privilegovaného přístupu ve finančních subjektech
EU GDPR	Článek 32	Přiměřená správa přístupu k ochraně osobních údajů
COBIT 2019	DSS05.03, DSS05.04	zřizování přístupu, odebírání přístupových oprávnění a pravidelný přezkum uživatelských přístupů

1. Účel

1.1 Tato politika stanoví pravidla pro správu uživatelských účtů a přístupových práv bezpečným, konzistentním a dohledatelným způsobem. Zajišťuje, aby k systémům a datům měli přístup pouze oprávnění uživatelé a aby rozsah přístupu odpovídal jejich roli a odpovědnostem.

1.2 Účinná správa účtů a oprávnění je nezbytná pro předcházení neoprávněnému přístupu, minimalizaci vnitřních hrozeb a zajištění souladu s ISO/IEC 27001, GDPR a dalšími regulatorními požadavky.

1.3 Tato politika umožňuje organizaci přiřadit vlastnictví a odpovědnost za používání účtů, monitorovat a auditovat eskalace oprávnění a bezpečně zakázat nebo odebrat přístup, pokud již není potřebný.

1.4 Dále chrání obchodní činnost před provozními chybami nebo zneužitím způsobenými nadměrným nebo nemonitorovaným přístupem a pomáhá snižovat riziko náhodného úniku dat, zneužití oprávnění nebo nesouladu s regulatorními požadavky.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny zaměstnance, stážisty, dodavatele a uživatele třetích stran s přístupem k IT systémům organizace

2.1.2 všechny systémy, zařízení, služby a platformy spravované organizací nebo jejím jménem, včetně cloudových platforem, lokální infrastruktury a nástrojů třetích stran

2.2 Zahrnuje všechny typy uživatelských účtů, včetně:

2.2.1 pojmenovaných uživatelských účtů (např. e-mailové účty, systémová přihlášení)

2.2.2 administrátorských a systémových účtů

2.2.3 dočasných, hostovských nebo přístupových údajů třetích stran

2.2.4 servisních účtů používaných aplikacemi nebo automatizačními systémy

2.3 Politika se uplatňuje v celém životním cyklu účtu – od vytvoření a schválení po změnu, monitorování a deaktivaci. To zahrnuje počáteční zřizování přístupu při nástupu, přezkumy přístupu při změnách rolí a odebrání přístupu při ukončení.

3. Cíle

3.1 Přiřadit všem uživatelům systémů jedinečné a dohledatelné identity, zajistit odpovědnost a vyloučit používání sdílených přihlašovacích údajů.

3.2 Uplatňovat zásadu minimálních oprávnění a zajistit, aby uživatelům byla udělena pouze minimální úroveň přístupu nezbytná pro výkon jejich pracovních povinností.

3.3 Předcházet neoprávněnému přístupu k citlivým systémům nebo datům prostřednictvím jasně dokumentovaných schvalovacích a přezkumných procesů.

3.4 Zajistit včasnou deaktivaci uživatelských účtů, jakmile již nejsou vyžadovány, např. při ukončení pracovního poměru, dokončení smlouvy nebo změně role.

3.5 Udržovat bezpečné prostředí připravené na audit prostřednictvím dokumentace všech změn účtů, schválení a pravidelných přezkumů.

3.6 Zajistit, aby zvýšení oprávnění bylo přísně řízeno, nezávisle schvalováno a protokolováno a aby zvýšený přístup byl neprodleně odebrán, jakmile již není potřebný.

4. Role a odpovědnosti

4.1 generální ředitel (GM)

4.1.1 Nese celkovou odpovědnost za uplatňování této politiky.

4.1.2 Zajišťuje, aby postupy správy účtů byly v souladu s požadavky certifikace ISO/IEC 27001 a příslušnými právními povinnostmi (např. GDPR).

4.1.3 Musí být neprodleně informován o jakémkoli neoprávněném přístupu, bezpečnostním incidentu nebo porušení politiky souvisejícím s uživatelskými účty.

4.1.4 Dohlíží na přezkumy politiky, audity a kroky k prosazování této politiky.

4.2 Vedoucí IT nebo externí poskytovatel IT služeb

4.2.1 Odpovídá za technickou implementaci kontrol účtů a oprávnění napříč systémy používanými organizací.

4.2.2 Smí zřizovat přístup, měnit a deaktivovat uživatelské účty pouze na základě dokumentovaných schválení.

4.2.3 Musí vynucovat požadavky na složitost hesel, časový limit uzamčení obrazovky, vícefaktorové ověřování (MFA), je-li dostupné, a protokolování systémů.

4.2.4 Musí uchovávat zabezpečené záznamy o všech schváleních přístupu, vlastnictví účtů, eskalacích oprávnění a odebrání přístupu.

4.2.5 Musí monitorovat neoprávněné nebo osiřelé účty a zjištěné nesrovnalosti hlásit GM.

[... 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 nejméně jednou ročně přezkoumána GM a Vedoucím IT, aby byl zajištěn soulad s:

9.1.1 aktuálními opatřeními a pokyny ISO/IEC 27001:2022

9.1.2 regulatorními aktualizacemi (např. GDPR, DORA, NIS2)

9.1.3 změnami v systémech, službách nebo struktuře organizace

9.2 Přezkumy musí být provedeny také po:

9.2.1 významných bezpečnostních incidentech nebo zjištěních auditu

9.2.2 zásadních změnách IT systémů nebo architektury účtů

9.2.3 zavedení nových platforem vyžadujících integraci řízení přístupu

9.3 Všechny změny musí být schváleny GM a srozumitelně komunikovány dotčeným pracovníkům.

10. Související politiky a vazby

10.1 P2S – Politika rolí a odpovědností v oblasti správy a řízení: stanoví odpovědnost a rozhodovací pravomoci pro schvalování přístupu a dohled.

10.2 P4S – Politika řízení přístupu: upravuje uplatňování řízení přístupu napříč systémy a metody ověřování.

10.3 P7S – Politika nástupu a ukončení: zajišťuje, aby vytváření a rušení účtů bylo součástí personálních změn řízených HR.

10.4 P8S – Politika povědomí o bezpečnosti informací a školení: školí uživatele v bezpečných postupech práce s účty a očekávaném způsobu jejich používání.

10.5 P30S – Politika reakce na incidenty (P30): vymezuje kroky, které mají být přijaty, pokud zneužití účtu vede k porušení bezpečnosti nebo neoprávněnému zpřístupnění.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 5.3: vyžaduje, aby role a odpovědnosti v oblasti bezpečnosti informací byly jasně přiřazeny a uplatňovány.

11.1.2 Článek 8.1: provozní plánování a řízení musí zahrnovat správu přístupu uživatelů.

11.2 ISO/IEC 27002

11.2.1 Opatření 8.2: stanoví technická a procesní opatření pro přidělování, přezkum a odebírání zvýšených oprávnění.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: vyžaduje zřizování účtů, monitorování a odebrání přístupu na základě definovaných rolí a procesů.

11.3.2 AC-5: řeší oddělení povinností s cílem zabránit střetu nebo zneužití oprávnění.

11.3.3 AC-6: vyžaduje uplatňování zásady minimálních oprávnění na všechna přístupová práva.

11.4 EU GDPR

11.4.1 Článek 32: vyžaduje přiměřenou správu přístupu k ochraně osobních údajů před neoprávněným přístupem nebo změnou.

11.5 EU NIS

11.5.1 Článek 21(2)(d): vyžaduje správu přístupu uživatelů jako součást hlavních bezpečnostních opatření pro základní a důležité subjekty.

11.6 EU DORA

11.6.1 Článek 9(2)(b): vyžaduje, aby finanční subjekty zavedly správu přístupu, která omezuje a monitoruje privilegovaná práva.

11.7 COBIT 2019

11.7.1 DSS05.03: stanoví zřizování přístupu a odebírání přístupových oprávnění uživatelů jako součást správy a řízení IT.

11.7.2 DSS05.04: požaduje průběžný přezkum a sladění uživatelského přístupu s rolemi v organizaci.