					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P11S					Názov dokumentu: **Politika správy používateľských účtov a oprávnení**							
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 5.3, 8	Roly, zodpovednosti a prevádzkové plánovanie a riadenie v oblasti riadenia prístupu používateľov
ISO/IEC 27002:2022	Kontrola 8	Kontroly prideľovania, preskúmavania a odoberania zvýšených oprávnení
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Zriaďovanie účtov, monitorovanie, zásada minimálnych oprávnení a oddelenie povinností
EÚ NIS2	Článok 21(2)(d)	riadenie prístupu používateľov pre základné a dôležité subjekty
EÚ DORA	Článok 9(2)(b)	riadenie privilegovaného prístupu vo finančných subjektoch
COBIT 2019	DSS05.03, DSS05.04	zriaďovanie prístupu, odoberanie prístupových práv a pravidelné preskúmavanie používateľských prístupov
EÚ GDPR	Článok 32	primerané kontroly prístupu na ochranu osobných údajov

1. Účel

1.1 Táto politika stanovuje pravidlá správy používateľských účtov a prístupových práv bezpečným, konzistentným a sledovateľným spôsobom. Zabezpečuje, aby mali k systémom a údajom prístup len oprávnení používatelia a aby bol tento prístup primeraný ich roli a zodpovednostiam.

1.2 Účinná správa účtov a oprávnení je nevyhnutná na predchádzanie neoprávnenému prístupu, minimalizáciu vnútorných hrozieb a zabezpečenie súladu s ISO/IEC 27001, GDPR a ďalšími regulačnými požiadavkami.

1.3 Táto politika umožňuje organizácii priradiť vlastníctvo a zodpovednosť za používanie účtov, monitorovať a auditovať eskalácie oprávnení a bezpečne deaktivovať alebo odobrať prístup, keď už nie je potrebný.

1.4 Zároveň chráni prevádzku organizácie pred prevádzkovými chybami alebo zneužitím spôsobeným nadmerným alebo nemonitorovaným prístupom a pomáha znižovať riziko náhodného úniku údajov, zneužitia oprávnení alebo nesúladu s predpismi.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých zamestnancov, stážistov, zmluvných pracovníkov a používateľov tretích strán s prístupom do IT systémov organizácie,

2.1.2 všetky systémy, zariadenia, služby a platformy spravované organizáciou alebo v jej mene vrátane cloudových platforiem, lokálnej infraštruktúry a nástrojov tretích strán.

2.2 Zahŕňa všetky typy používateľských účtov vrátane:

2.2.1 pomenovaných používateľských účtov (napr. e-mailové účty, systémové prihlásenia),

2.2.2 administrátorských účtov a systémových účtov,

2.2.3 dočasných, hosťovských alebo prístupových poverení tretích strán,

2.2.4 servisných účtov používaných aplikáciami alebo automatizačnými systémami.

2.3 Politika sa uplatňuje počas celého životného cyklu účtu od vytvorenia a schválenia až po zmenu, monitorovanie a deaktiváciu. To zahŕňa počiatočné zriaďovanie prístupu počas procesu nástupu, revíziu prístupových práv pri zmenách rolí a zrušenie prístupových oprávnení počas ukončenia pracovného pomeru alebo spolupráce.

3. Ciele

3.1 Priradiť všetkým používateľom systémov jedinečné a sledovateľné identity, čím sa zabezpečí zodpovednosť za konanie a vylúči sa používanie zdieľaných prihlasovacích údajov.

3.2 Uplatňovať zásadu minimálnych oprávnení tak, aby používateľom bola pridelená len minimálna úroveň prístupu nevyhnutná na výkon ich pracovných povinností.

3.3 Predchádzať neoprávnenému prístupu k citlivým systémom alebo údajom prostredníctvom jasne zdokumentovaných procesov schvaľovania a preskúmavania.

3.4 Zabezpečiť včasnú deaktiváciu používateľských účtov, keď už nie sú potrebné, napríklad pri ukončení pracovného pomeru, ukončení zmluvy alebo zmene roly.

3.5 Udržiavať bezpečné prostredie pripravené na audit dokumentovaním všetkých zmien účtov, schválení a pravidelných preskúmaní.

3.6 Zabezpečiť, aby zvýšenie oprávnení podliehalo prísnej kontrole, nezávislému schváleniu a logovaniu a aby bol zvýšený prístup bezodkladne odobratý, keď už nie je potrebný.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie celkovú zodpovednosť za uplatňovanie tejto politiky.

4.1.2 Zabezpečuje, aby postupy správy účtov boli v súlade s požiadavkami na certifikáciu podľa ISO/IEC 27001 a príslušnými zákonnými povinnosťami (napr. GDPR).

4.1.3 Musí byť bezodkladne informovaný o každom neoprávnenom prístupe, bezpečnostnom incidente alebo porušení politiky súvisiacom s používateľskými účtami.

4.1.4 Dohliada na preskúmania politiky, audity a opatrenia pri porušení.

4.2 Vedúci IT alebo externý poskytovateľ IT služieb

4.2.1 Zodpovedá za technickú implementáciu kontrol účtov a oprávnení naprieč systémami používanými organizáciou.

4.2.2 Musí zriaďovať, upravovať a deaktivovať používateľské účty výlučne na základe zdokumentovaných schválení.

4.2.3 Musí uplatňovať požiadavky na zložitosť hesiel, časový limit uzamknutia obrazovky, viacfaktorové overovanie (MFA), ak je dostupné, a systémové logovanie.

4.2.4 Musí viesť bezpečné záznamy o všetkých schváleniach prístupu, vlastníctve účtov, eskaláciách oprávnení a zrušeniach prístupových oprávnení.

4.2.5 Je povinný monitorovať neoprávnené alebo osirelé účty a hlásiť nezrovnalosti GM.

[... 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 Túto politiku musia GM a vedúci IT preskúmať najmenej raz ročne, aby zabezpečili súlad s:

9.1.1 aktuálnymi kontrolami a usmerneniami ISO/IEC 27001:2022,

9.1.2 regulačnými aktualizáciami (napr. GDPR, DORA, NIS2),

9.1.3 zmenami v systémoch, službách alebo štruktúre organizácie.

9.2 Preskúmanie sa musí vykonať aj po:

9.2.1 významných bezpečnostných incidentoch alebo auditných zisteniach,

9.2.2 významných zmenách v IT systémoch alebo architektúre účtov,

9.2.3 zavedení nových platforiem vyžadujúcich integráciu riadenia prístupu.

9.3 Všetky zmeny musí schváliť GM a musia byť zrozumiteľne komunikované dotknutým zamestnancom.

10. Súvisiace politiky a väzby

10.1 P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: stanovuje zodpovednosť a rozhodovacie právomoci pre schvaľovanie prístupov a dohľad.

10.2 P4S – Politika riadenia prístupu: upravuje uplatňovanie riadenia prístupu v rámci systémov a metódy autentifikácie.

10.3 P7S – Politika nástupu a ukončenia: zabezpečuje, aby vytváranie a rušenie účtov bolo súčasťou personálnych zmien riadených HR.

10.4 P8S – Politika povedomia a školenia o informačnej bezpečnosti: školí používateľov v oblasti bezpečných postupov pri používaní účtov a očakávaného správania.

10.5 P30S – Politika reakcie na incidenty (P30): definuje kroky, ktoré sa majú prijať, ak zneužitie účtu vedie k narušeniu bezpečnosti alebo neoprávnenému sprístupneniu.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.3: vyžaduje, aby roly a zodpovednosti v oblasti informačnej bezpečnosti boli jasne pridelené a uplatňované.

11.1.2 Kapitola 8.1: prevádzkové plánovanie a riadenie musí zahŕňať riadenie prístupu používateľov.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.2: uvádza technické a procesné kontroly pre prideľovanie, preskúmavanie a odoberanie zvýšených oprávnení.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: vyžaduje zriaďovanie účtov, monitorovanie a zrušenie prístupových oprávnení na základe definovaných rolí a procesov.

11.3.2 AC-5: rieši oddelenie povinností s cieľom predchádzať konfliktu alebo zneužitiu oprávnení.

11.3.3 AC-6: vyžaduje uplatňovanie zásady minimálnych oprávnení na všetky prístupové práva.

11.4 GDPR EÚ

11.4.1 Článok 32: vyžaduje primerané kontroly prístupu na ochranu osobných údajov pred neoprávneným prístupom alebo zmenou.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(d): vyžaduje riadenie prístupu používateľov ako súčasť základných bezpečnostných kontrol pre základné a dôležité subjekty.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 9(2)(b): vyžaduje, aby finančné subjekty implementovali kontroly prístupu, ktoré obmedzujú a monitorujú privilegované práva.

11.7 COBIT 2019

11.7.1 DSS05.03: špecifikuje zriaďovanie prístupu a odoberanie prístupových práv používateľov ako súčasť správy a riadenia IT.

11.7.2 DSS05.04: vyžaduje priebežné preskúmavanie a zosúladenie používateľských prístupov s organizačnými rolami.