					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P11					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**

Zosúladené s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 6.1.3, Kapitola 8	-
ISO/IEC 27002:2022	Kontroly 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	-
Nariadenie EÚ GDPR	Články 5(1)(f), 32; odôvodnenie 39	-
Smernica EÚ NIS2	Články 21(2)(a, d), 21(3)	-
Nariadenie EÚ DORA	Články 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Účel

1 Táto politika stanovuje záväzné kontroly pre správu používateľských účtov a oprávnení vo všetkých informačných systémoch a službách. Zabezpečuje, aby bol prístup k zdrojom organizácie udeľovaný na základe overenej identity, odôvodnenej potreby vyplývajúcej z pracovnej roly a v súlade so zásadou minimálnych oprávnení a oddelenia povinností.

1.1 Podporuje záväzok organizácie k informačnej bezpečnosti zavedením štruktúrovaných, auditovateľných procesov pre zriaďovanie účtov, prideľovanie oprávnení, monitorovanie používania a odoberanie prístupových práv k účtom.

1.2 Táto politika je kľúčová pre znižovanie rizika neoprávneného prístupu, zneužitia oprávnení, vnútorných hrozieb a nesúladu s príslušnými regulačnými rámcami.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetkých zamestnancov, zmluvných dodávateľov, poskytovateľov služieb tretích strán, konzultantov a ďalšie osoby, ktorým bol udelený prístup k IT zdrojom, aplikáciám alebo údajom organizácie.

2.2 Upravuje všetky systémy a prostredia, v ktorých sa uplatňujú mechanizmy autentifikácie používateľov a riadenia prístupu, vrátane najmä:

2.2.1 podnikových aplikácií a databáz,

2.2.2 cloudových platforiem a prostredí SaaS,

2.2.3 operačných systémov a administrátorských konzol,

2.2.4 nástrojov vzdialeného prístupu a VPN,

2.2.5 systémov riadenia identít a prístupu (IAM).

2.3 Politika zahŕňa štandardné aj privilegované používateľské účty a pokrýva kontroly nad:

2.3.1 vytváraním, úpravou a deaktiváciou účtov,

2.3.2 eskaláciou oprávnení a delegovaním,

2.3.3 riadením a monitorovaním relácií,

2.3.4 metódami autentifikácie a správou prihlasovacích údajov.

3. Ciele

3.1 Zabezpečiť, aby boli všetky používateľské účty jednoznačne identifikovateľné, riadne autorizované a prideľované len po formálnom overení potreby.

3.2 Uplatňovať zásadu minimálnych oprávnení a predchádzať zbytočnému alebo nadmernému prístupu zavedením prísnych kontrol pri prideľovaní a používaní privilegovaných účtov.

3.3 Vyžadovať včasnú aktualizáciu stavu účtov na základe zmien pracovného zaradenia alebo roly vrátane okamžitej deaktivácie pri ukončení pracovného alebo zmluvného vzťahu.

3.4 Umožniť proaktívnu detekciu a nápravu neaktívnych, zneužívaných alebo neoprávnených účtov prostredníctvom logovania, preskúmaní a automatizácie.

3.5 Zachovať súlad s ISO/IEC 27001:2022 a súvisiacimi normami a plniť povinnosti podľa príslušných právnych a regulačných rámcov, ako sú GDPR, NIS2, DORA a COBIT 2019.

4. Roly a zodpovednosti

4.1 Riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej uplatňovanie v celej organizácii.

4.1.2 Preskúmava a schvaľuje všetky formálne výnimky alebo prípady núdzového prístupu.

4.1.3 Informuje vrcholový manažment o auditných zisteniach súvisiacich s účtami a eskaluje riziká.

4.2 Manažér riadenia prístupu / IT administrátor

4.2.1 Udržiava a prevádzkuje technické kontroly na riadenie životného cyklu používateľských účtov.

4.2.2 Vykonáva zriaďovanie prístupu, odoberanie prístupových práv a správu oprávnení na základe schválenej požiadavky.

4.2.3 Vedie autoritatívny register všetkých používateľských účtov, ich stavu a úrovní oprávnení.

4.2.4 Podporuje audity a preskúmania súladu prostredníctvom logov a správ o aktivitách.

[... 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 Táto politika sa musí preskúmať najmenej raz ročne alebo pri významných zmenách týkajúcich sa:

9.1.1 organizačnej štruktúry alebo podnikových procesov,

9.1.2 IT systémov, platforiem identít alebo metód prístupu,

9.1.3 regulačných alebo zmluvných požiadaviek súvisiacich s riadením identít a prístupu.

9.2 Za iniciovanie procesu preskúmania a koordináciu spätnej väzby zainteresovaných strán zodpovedá riaditeľ informačnej bezpečnosti (CISO) v spolupráci s manažérom riadenia prístupu.

9.3 Mimoriadne preskúmania môžu byť vyvolané:

9.3.1 bezpečnostnými incidentmi súvisiacimi so zneužitím účtov,

9.3.2 auditnými zisteniami poukazujúcimi na nedostatky v riadení životného cyklu účtov,

9.3.3 nasadením nových nástrojov na správu identít alebo privilegovaného prístupu.

9.4 Aktualizácie tejto politiky musia byť:

9.4.1 predmetom riadenia verzií a zaznamenané v knižnici dokumentácie ISMS,

9.4.2 oznámené všetkým relevantným zainteresovaným stranám vrátane vedúcich oddelení, IT prevádzky a HR,

9.4.3 podporené aktualizovanými školiacimi materiálmi a procesnými príručkami.

9.5 Všetky zmeny musí schváliť výkonný manažment alebo Riadiaci výbor pre informačnú bezpečnosť a musia byť zaznamenané na účely auditu.

10. Súvisiace politiky a väzby

10.1 Táto politika je prevádzkovo prepojená s nasledujúcimi súvisiacimi politikami v rámci ISMS a je nimi podporovaná:

10.1.1 P4 Politika riadenia prístupu: stanovuje nadradené zásady a mechanizmy riadenia prístupu vrátane pravidlovo riadených a rolovo riadených kontrol.

10.1.2 P7 Politika nástupu a ukončenia: stanovuje procesné kroky na zriadenie a ukončenie používateľského prístupu v súlade s úkonmi HR.

10.1.3 P8 Politika povedomia a školenia v oblasti informačnej bezpečnosti: posilňuje zodpovednosti používateľov za bezpečnosť účtov a ochranu prihlasovacích údajov.

10.1.4 P13 Politika klasifikácie a označovania údajov: usmerňuje úrovne prístupu na základe klasifikácie údajov a zabezpečuje, aby hranice oprávnení zodpovedali úrovni citlivosti.

10.1.5 P22 Politika logovania a monitorovania: zabezpečuje zhromažďovanie auditných stôp pre všetky činnosti súvisiace s účtami a ich preskúmavanie na účely detekcie anomálií alebo neoprávneného používania.

10.1.6 P30 Politika reakcie na incidenty: upravuje eskaláciu, zamedzenie šírenia a činnosti po incidente v prípadoch zneužitia oprávnení alebo neoprávnenej aktivity účtov.

10.2 Každá z týchto politík sa uplatňuje spoločne s cieľom zabezpečiť ucelený rámec riadenia identít a prístupu založený na riziku v celej organizácii.

11. Referenčné normy a rámce

11.1 Táto politika je zosúladená s medzinárodne uznávanými štandardmi kybernetickej bezpečnosti a regulačnými rámcami, ktoré vyžadujú bezpečné riadenie identít, prístupu a oprávnení ako základnú súčasť informačnej bezpečnosti organizácie.

11.2 ISO/IEC 27001:

11.2.1 Kapitola 6.1.3 vyžaduje, aby organizácie určovali, hodnotili a ošetrovali riziká informačnej bezpečnosti, čím sa riadenie prístupu a oprávnení stáva formálnou kontrolou založenou na riziku, začlenenou do procesu plánovania ISMS.

11.2.2 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: posilňuje implementáciu technických a procesných ochranných opatrení, ktoré upravujú používateľský a privilegovaný prístup.

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

11.3.1 Kontrola 5.15 – riadenie prístupu používateľov: podporuje formálne procesy pre zriaďovanie prístupu, autorizáciu prístupu a pravidelné preskúmanie prístupových práv.

11.3.2 Kontrola 5.16 – správa identít: stanovuje jedinečnosť identít, kontroly životného cyklu a uplatňovanie bezpečnej autentifikácie.

11.3.3 Kontrola 5.17 zabezpečuje, že prideľovanie a používanie práv privilegovaného prístupu je prísne riadené, sledovateľné a zosúladené so zásadou minimálnych oprávnení počas celého životného cyklu používateľského účtu.

11.3.4 Kontrola 5.18 – práva privilegovaného prístupu: je plne pokrytá prideľovaním oprávnení na základe rolí, auditovaním a požiadavkami na schvaľovanie zvýšeného prístupu.

11.4 Tieto kontroly usmerňujú štruktúrovanú implementáciu registrácie a zrušenia registrácie účtov, oddelenia oprávnení a používania autentifikačných údajov. Politika uplatňuje správu životného cyklu identít, just-in-time prístup a monitorovanie zvýšených relácií s cieľom predchádzať neoprávnenému používaniu systému.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (politika riadenia prístupu) a AC-2 (správa účtov): sú mapované prostredníctvom požiadaviek politiky na schvaľovanie prístupu, mapovanie rolí a auditovanie používateľských účtov.

11.5.2 AC-5 (oddelenie povinností) a AC-6 (zásada minimálnych oprávnení): sú naplnené prostredníctvom obmedzenia oprávnení, zosúladenia s pracovnou rolou a dvojitého schvaľovania pri úlohách s vysokým rizikom.

11.5.3 IA-2 až IA-5 (identifikácia a autentifikácia): sú uplatňované prostredníctvom silných mechanizmov autentifikácie, pravidiel životného cyklu prihlasovacích údajov a požiadaviek na MFA.

11.5.4 AU-2, AU-12 (auditné logovanie a analýza): sú pokryté zaznamenávaním relácií a monitorovaním privilegovaných aktivít v citlivých prostrediach.

11.6 Nariadenie EÚ GDPR (2016/679):

11.6.1 Článok 32 – bezpečnosť spracúvania: vyžaduje kontroly prístupu a mechanizmy overovania identity na ochranu osobných údajov. Táto požiadavka je naplnená povinným schvaľovaním účtov, revíziami oprávnení a silnými ochrannými opatreniami autentifikácie.

11.6.2 Článok 5(1)(f) – integrita a dôvernosť: zabezpečuje, aby k osobným údajom pristupovali len oprávnení používatelia s legitímnymi rolami, čo je posilnené uplatňovaním správy účtov.

11.6.3 Odôvodnenie 39: požaduje jasné obmedzenie prístupu a preukázateľnú zodpovednosť; táto politika podporuje úplnú sledovateľnosť identít používateľov a prideľovania oprávnení.

11.7 Smernica EÚ NIS2 (2022/2555):

11.7.1 Článok 21(2)(a, d): vyžaduje, aby subjekty uplatňovali politiky správy prístupu a bezpečné nakladanie s prihlasovacími údajmi a privilegovanými reláciami, čo je podporené prostredníctvom kontrol zriaďovania prístupu, monitorovania a výnimiek podľa tejto politiky.

11.7.2 Článok 21(3): podporuje disciplínu prístupu a vysokú dôveryhodnosť identity v kritických odvetviach, čo je naplnené používaním jedinečných identifikátorov, RBAC a časovo obmedzeného zvýšeného prístupu.

11.8 Nariadenie EÚ DORA (2022/2554):

11.8.1 Článok 5 – správa a riadenie a kontrola IKT: vyžaduje formalizované procesy na správu používateľov systémov IKT, ktoré sú pokryté prostredníctvom zdokumentovaného zriaďovania prístupu, deaktivácie a ošetrenia výnimiek.

11.8.2 Článok 9 – riadenie rizík IKT: usmerňuje organizácie zabezpečiť systémy prostredníctvom obmedzení prístupu a monitorovania, čo je riešené prostredníctvom MFA, logovania privilegovaného prístupu a centralizovaných preskúmaní.

11.9 COBIT 2019:

11.9.1 DSS01 – riadené operácie: podporuje uplatňovanie štandardizovaných prevádzkových kontrol vrátane riadenia životného cyklu používateľských účtov a dokumentácie prístupu.

11.9.2 DSS05 – riadené bezpečnostné služby: odráža bezpečnú správu používateľských a systémových oprávnení a podporuje zmierňovanie rizík prostredníctvom zásady minimálnych oprávnení a overovania auditnej stopy.

11.9.3 APO13 – riadená bezpečnosť: vyžaduje riadenie prístupu naprieč digitálnymi aktívami, čo sa napĺňa prostredníctvom formalizovaných postupov autorizácie účtov a rolí s požiadavkami na pravidelné preskúmanie.