10-1-12 Informacinių sistemų prieigos teisių politika

Galioja nuo: 2025-03-05	Leidimas: 1
Politikos rengėjas: IT platformų grupės vadovas Andrius Dukšta, Informacinių sistemų skyrius	
Politikos tvirtintojas: *Generalinis direktorius*	
Publikuojama: *Privačiai* ☐ *Viešai* ☒	

1. TIKSLAS

Ši politika nustato prieigos kontrolės reikalavimus informacinėms sistemoms, siekiant užtikrinti, kad prieigą turėtų tik įgalioti naudotojai, laikantis ISO 27001:2022 A priedo 5.18 p. (Prieigos teisės) reikalavimų ir kitų taikomų saugumo standartų.

2. TAIKYMO SRITIS

Ši politika taikoma visiems darbuotojams, rangovams, trečiųjų šalių paslaugų teikėjams ir kitiems asmenims, kuriems reikia prieigos prie organizacijos informacinių sistemų, tinklų ir duomenų.

3. POLITIKOS NUOSTATOS

Organizacija įgyvendina prieigos kontrolės mechanizmus, kad apsaugotų informacijos išteklius nuo neteisėtos prieigos, pakeitimų ar atskleidimo. Prieiga bus suteikiama laikantis minimalaus būtinumo ir reikalingumo žinoti principų.

4. ATSAKOMYBĖS

Informacijos saugumo vadovas (ISM): Užtikrina politikos laikymąsi ir reguliariai peržiūri naudotojų prieigos teises.

Sistemų savininkai: Tvirtina naudotojų prieigą pagal verslo poreikius.

IT administratorius: Vykdo naudotojų įgaliojimą ir pašalinimą pagal darbo santykių statusą.

Darbuotojai ir naudotojai: Atsakingi už saugumo užtikrinimą ir neteisėtos prieigos pranešimą.

5. PRIEIGOS KONTROLĖS PRINCIPAI

5.1 Naudotojų prieigos valdymas

- Privalomas naudotojų registracijos ir pašalinimo procesas.
- Prieigos teisės suteikiamos pagal naudotojo vaidmenį ir mažiausios privilegijos principą.
- Prieigą prie sistemų privalo patvirtinti sistemos savininkas arba skyriaus vadovas.
- Periodinė prieigos peržiūra (ne rečiau kaip kas 6 mėnesius) siekiant patvirtinti prieigos būtinumą.

5.2 Privilegijuotos prieigos valdymas (PAM)

- Privilegijuotos paskyros (pvz., administratorius, root, supernaudotojas) turi būti ribojamos ir stebimos.
- Privilegijuotai prieigai privaloma daugiapakopė autentifikacija (MFA).
- Bendrų privilegijuotų paskyrų naudojimas draudžiamas, išskyrus būtinus atvejus, kai visos operacijos yra registruojamos.

5.3 Nuotolinės prieigos kontrolė

- Nuotolinė prieiga leidžiama tik naudojant saugų VPN ar kitus užšifruotus ryšius.
- Privaloma MFA ir prieigos registravimas bei stebėsena.
- Nenaudojama nuotolinė prieiga turi būti nedelsiant išjungta.

5.4 Trečiųjų šalių ir laikinos prieigos valdymas

- Trečiųjų šalių ar rangovų prieiga turi būti ribota pagal poreikį ir laiką.
- Trečiųjų šalių prieiga privalo būti peržiūrima ir pašalinama pasibaigus projektui.

6. AUTENTIFIKAVIMO IR SLAPTAŽODŽIŲ POLITIKA

- Slaptažodžiai turi būti ne trumpesni kaip 8 simbolių ir turėti didžiųjų, mažųjų raidžių, skaičių bei specialiųjų simbolių.
- Sistemos numatytuosius slaptažodžius būtina pakeisti nedelsiant po pirmo prisijungimo.
- Slaptažodžiai privalo būti užšifruoti ir niekada nesaugomi atvirame tekste.
- Po 5 nesėkmingų bandymų paskyra turi būti laikinai užblokuojama.

7. PRIEIGOS STEBĖSENA IR REGISTRAVIMAS

- Visi prieigos bandymai – tiek sėkmingi, tiek nesėkmingi – turi būti registruojami ir stebimi.
- Žurnalo duomenys saugomi mažiausiai 12 mėnesių audito ir atitikties tikslais.
- Privaloma konfigūruoti saugumo perspėjimus apie neteisėtus prisijungimus.

8. PRIEIGOS NUTRAUKIMAS IR PAŠALINIMAS

- Darbuotojo išėjimo ar rolės pasikeitimo atveju visos prieigos teisės turi būti pašalintos per 24 valandas.
- IT skyrius turi patvirtinti visų paskyrų išjungimą.
- Prieigos įrašai turi būti periodiškai tikrinami, siekiant nustatyti neaktyvias paskyras.

9. POLITIKOS PERŽIŪRA IR LAIKYMASIS

Ši politika peržiūrima kasmet arba esant reikšmingiems verslo procesų pokyčiams. Politikos nesilaikymas gali lemti drausmines priemones, įskaitant darbo santykių nutraukimą.

LEIDIMŲ ISTORIJA

Leidimo Nr.	Parengimo data	Leidimo aprašymas	Leidimo priežastis	Leidimą parengė (vardas, pavardė, pareigos)
1.	2025-03-05	Išleistas dokumentas	Naujas	Andrius Dukšta, IT platformų grupės vadovas