KOCSORD POLGÁRMESTERI HIVATALÁNAK INFORMATIKAI ENGEDÉLYEZÉSI ÉS JOGOSULTSÁGI SZABÁLYZATA

Kelt: Kocsord, 2020. április 01.

Dr. Gellért-Kovács Adrienn
jegyző

Verzió: 1.0

Tartalomjegyzék

1. Általános rendelkezések

1.1. A szabályzat célja

Jelen szabályzat rendelkezik Kocsord Polgármesteri Hivatalának (továbbiakban: Hivatal) információs rendszereinek a szerepkörök és jogosultságok tekintetében támasztott elvárásairól, melyeket rendszertechnikailag meg kell valósítani.

1.2. A szabályzat hatálya

A szabályzat érvényessége kiterjed a Hivatal valamennyi szervezeti egységére, funkciójára és folyamatára.

1.3. A jogosultságkezelés céljai

a) a Hivatalnál csak az arra jogosult személyek rendelkezhetnek hozzáféréssel a rendszerekhez és az információkhoz;
b) a vezetőknek és az alkalmazottaknak ismerniük kell a feladatokat és a szükséges jogokat;
c) valamennyi felhasználó személyre szóló felhasználói jogosultságot kell, hogy rendelkezzen;
d) kerülni kell az ellentmondó vagy egymást kioltó jogosultságokat, szerepköröket;
e) a jogosultságok igénylése, engedélyezése, visszavonása dokumentált kell, hogy legyen;

1.4. Definíciók

1. *felhasználói fiókok:* a felhasználói fiókok a hálózatokon vagy alkalmazásokon belül a felhasználó egyértelmű beazonosítására szolgál.

2. *szerepkörök:* tevékenységeik gyakorlásához a hivatali dolgozóknak feladataiknak megfelelő jogokra van szükségük. A csoportokban összefoglalt jogokat szerepköröknek nevezzük. Ez az összefoglalás csökkenti az operatív IT-kockázatokat és növeli a hatékonyságot a hozzáférési jogok adminisztrációja során

3. *szolgáltatás fiókok (service accountok):* a személyhez nem kötött felhasználó fiókokat szolgáltatás fióknak nevezzük. Elsősorban olyan funkciók és feladatok számára kerülnek bevetésre, amelyek nem igénylik a mindenkori felhasználó interaktív tevékenységét, hanem pl. az IT-rendszerek közötti adatcseréhez szükségesek

1.5. Felelősségek

1.5.1 A Hivatal vezetése

a) felelős a kritériumok meghatározásáért
b) kinevezi a fiók felelősöket, tevékenységüket felügyeli
c) dönt a szabályok elfogadásáról és a szükséges intézkedésekről
d) gondoskodik a szabályzás fontosságának tudatosításáról és annak betartatásáról

1.5.2 Az IT referens

a) felelős a jogosultságok kialakításáért, nyilvántartásáért és naprakészen tartásáért
b) javaslatokat tesz a szabályok módosítására
c) felelős a szükséges oktatások megtartásáért, megtartatásáért
d) kezdeményezi az éves rendszeres felülvizsgálatokat

1.5.3 A munkatársak

a) Felelős a közzétett, illetve számukra kiadott előírások betartásáért

2. A fiókkezelés szabályozása

2.1. A fiókkezeléssel kapcsolatos elvárások

a) a rendszerek és információk elérése csak sikeres beazonosítást követően válhat lehetővé.
b) minden felhasználónak önálló, személyre szóló fiókot kell kapnia, amely egyértelműen beazonosítható
c) tiltott a más személyek felé, ill. más személyek által történő továbbadás vagy felhasználás
d) a felhasználói fiókokat egységes névkonvenció szerint javasolt létrehozni
e) privilegizált jogosultságokhoz, azaz olyan jogosultságokhoz, amelyek a Hivatal szempontjából kritikus adattörzsekhez rendelkeznek hozzáféréssel, vagy amelyek IT-rendszerek rendszer-konfigurációját teszik lehetővé (pl. adminisztrátorok, adatbank-felhasználók vagy fejlesztők), külön felhasználói fiókot kell létesíteni, elkülönítve a normális jogosultságot igénylő feladatokhoz használt fióktól
f) minden szolgáltatás fiókot (service accountot) felelőshöz kell hozzárendelni, aki felelős a szolgáltatás fiók aktualizálásáért és törléséért, jelszavainak rendszeres megváltoztatásáért
g) biztosítani kell, hogy csak feljogosított dolgozók ismerjék a szolgáltatás fiókok (service accountok) jelszavát.
h) valamennyi felhasználói fiókot és annak módosítását dokumentálni kell. Ennek kapcsán figyelembe kell venni az ellenőrzési követelményeket is.

2.2. A fiókok elnevezési szabályai (névkonvenció)

A felhasználói fiókokat egyértelműen kell kiadni. Amennyiben technikailag lehetséges, úgy már a felhasználói elnevezésből világosan felismerhetőnek kell lennie, hogy az adott fiók rendelkezik-e privilegizált jogokkal (pl. „gipsz.j_admin"), továbbá az elnevezésből levezethetőnek kell lennie magának a felhasználónak (pl. „gipsz.j") vagy szolgáltatás fiók esetén a feladatkörnek (pl. "daily_backup") is.

2.3. Fiókok létrehozása, módosítása, törlése

A felhasználói fiókok igénylésére, létrehozására és módosítására alkalmas eljárás minden esetben engedélyezési folyamatot tesz szükségessé. Ennek az engedélyezési folyamatnak mindenkor nyomon követhetően dokumentáltnak kell lennie oly módon, hogy vizsgálat esetén rövid időn belül és hiánytalanul igazolásokat lehessen felmutatni.

A felhasználói fiókok igénylését és engedélyezését a területen belül **két különböző személynek kell végrehajtania.** A felhasználói fiókok kezelése a rendszergazda felelősségi köréhez tartozik.

Felhasználói fiókot csak olyan személyek részére szabad kiadni, akik elfogadják a Hivatal információbiztonsági szabályait. Az elfogadást írásos úton kell megadni és annak nyomon követően dokumentáltnak kell lennie, amely a szerződés mellékletét képezheti. Ez különösen a külső szolgáltatókra érvényes.

A már nem szükséges fiókokat lehetőleg azonnal, de legfeljebb 5 munkanapon belül inaktívvá kell változtatni és három hónap elteltével törölni kell. A törlés csak akkor megengedett, ha az üzlet szempontjából lényeges és megőrzés-köteles adatok ezzel nem mennek veszendőbe és ellenőrzési követelmények ezeket nem tiltják.

3. A jogosultságok szabályozása

3.1. A jogosultságokkal kapcsolatos elvárások

a) RBAC elv (role-based access control), (szerepkörökön alapuló hozzáférési ellenőrzés): a jogosultságokat lehetőleg csak szerepkörökön keresztül adjuk ki és kerüljük az egyéni joghozzárendeléseket. Amennyiben ez nem lehetséges, úgy az eltéréseket külön kell dokumentálni és az alkalmazásukat, valamint szükségességüket rendszeresen kell ellenőrizni.
b) legalacsonyabb privilégium elve: a mindenkori szerepkörhöz mindig csak azon jogosultságok kerülnek kiadásra, amelyekre a szerepkörnek a teljesítendő feladatkörön belül végzett tevékenységhez valóban szüksége van.
c) feladat- és/vagy funkció-szétválasztás elve: a hozzáférési jogok kiadásának a feladat- és/vagy funkció-szétválasztás elve szerint kell megtörténnie, azaz a szakterület részéről szakmailag meghatározott szétválasztásoknak a kiadott és rendszertechnikailag hozzárendelt jogokban kell visszatükröződniük.
d) kerülni kell az egymásnak ellentmondó, ill. egymást kioltó jogosultságokkal rendelkező szerepköröket. Az eltéréseket dokumentálni, indokolni és azokat kivételként engedélyezni kell.

3.2. A jogosultságok elnevezési szabályai (névkonvenció)

Valamennyi meghatározott szerepkört és jogosultságot egységes elnevezési szabály szerint kell névvel ellátni, amely szabály a hozzátartozó feladatterületeket és jogokat egyértelműen felismerhetővé teszi. Ez az előírás érvényes a szerepkörök és a jogosultságok rendszertechnikai leképezésére is, amennyiben ez technikailag lehetséges.

3.3. A szerepkörök és jogosultságok megváltoztatása

A szerepkörök és jogosultságok változtatását meghatározott eljárás szerint a változáskezelés keretében kell végrehajtani. Ennek során az alábbi folyamatokat kell figyelembe venni:

a) a mindenkori felhasználó belépése az adott feladatkörbe (pl. munkaviszony létesítése, osztályváltás vagy átszervezés következtében).
b) a mindenkori felhasználó kilépése az adott feladatkörből (pl. nyugdíjba vonuláskor, osztályváltás vagy átszervezés következtében).
c) változtatások a feladatkörben, amelyek következményeként változtatások válnak szükségessé a jogosultságokban, vagy amelyek következményeként jogosultságok kerülnek megszüntetésre.

A Munkaügynek és a szakterületnek kell funkciójuk keretében valamennyi személyi változást és a jogosultságok ebből eredő változásait a felelős adminisztrátorok felé a jogosultságok minél korábbi illesztése érdekében közvetlenül lejelenteni.

Ennek során főként azt kell biztosítani, hogy a már nem szükséges jogosultságok rövid időn belül bevonásra kerüljenek, azaz amint azokra a mindenkori feladatkörön belüli teljesítéshez már nincs szükség.

3.4. A szerepkörök és jogosultságok ellenőrzése

Valamennyi szerepkört és kiadott jogosultságot legalább évente egy alkalommal kell felülvizsgálni. A vezetők kötelesek meggyőződni a meghonosított szerepkörök megfelelőségéről, a szerepkörök hozzárendelésének megfelelőségéről és esetleg a felhasználók járulékos egyéni jogosultságainak helyességéről. Az eltéréseket jelenteni kell az IT referensnek.

4. Egyéb rendelkezések

4.1. Fiókok és jogosultságok dokumentálása

A rendszergazda a felhasználókról és jogosultságaikról nyilvántartást vezet, mely tartalmazza:

a) a jogosult nevét, szervezeti egységét
b) a jogosultság tárgyát vagy a szerepkört
c) a jogosultság időtartamát (ha szükséges)

4.2. Egyéb biztonsági követelmények, ajánlások

a) az információbiztonság garantálása céljából valamennyi hozzáférési kísérletet naplózni kell
b) többszöri sikertelen bejelentkezési kísérletet követően az érintett fiókot automatikusan zárolni kell (a zárolás feloldásának módja lehet automatikus, vagy manuális is)
c) az inaktív munkameneteket meghatározott idő után zárolni kell, vagy meg kell szakítani
d) minden szolgáltatás esetében törekedni kell a központosított hitelesítésre (pl. LDAP)
e) törekedés a 4 szem-elvre: a jogosultságok engedélyezése és azok rendszertechnikai felvétele legalább +1 fő ellenőrzése mellett történjen meg

4.3. Általános korlátozások

Az információs rendszer nem használható az alábbi tevékenységekre:

a) az érvényes magyar jogszabályokba ütköző cselekmények, mint pl.: a szerzői jogok megsértése; szoftverek szándékos és tudatos illegális használata, terjesztése, stb.
b) haszonszerzést célzó, közvetlen üzleti célú tevékenység, reklámok terjesztése
c) az információs rendszer, illetve erőforrásai szabályos működését megzavaró, veszélyeztető, vagy erőforrásait pazarló tevékenységek, mint pl.: kéretlen levelek, elektronikus játékok, stb.
d) az információs rendszer erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére irányuló bármilyen tevékenység
e) vallási, etnikai, politikai, erkölcsi vagy más jellegű érzékenységet sértő, másokra nézve sértő, esetleg másokat zaklató tevékenység (pl. szélsőséges nézeteket képviselő, fajgyűlölő, vagy pornográf anyagok megtekintése, tárolása, közzététele vagy továbbítása)

5. ASP rendszerre vonatkozó eljárásrend

5.1. ASP jogosultságkezelés

A szerződésben meghatározott tenant adminisztrátorok rendszerbe történő „felvite-lét" az ASP Központ végzi el az önkormányzat által megküldött adatlap alapján.

- A privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot osztanak. Ezt a tevékenységet az önkormányzati jegyző felelőssé-gi és hatáskörébe tartozóan tudják elvégezni.
- Egy önkormányzati fióknál (tenantnál) minimum egy felhasználó karbantartónak szükséges „lenni", ezt a rendszer figyeli (pl.: nem lehet zárolni, vagy elvenni tőle a jogot, ha csak egyedüli felhasználó karbantartó a tenantnál).
- A rendszer használata során elvárt, hogy a privilegizált joggal rendelkező mun-katársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használják.
- A privilegizált joghoz tartozó bejelentkezési azonosítót zárt borítékban, bizton-ságosan zárható helyen kell tárolni.

A tenant adminisztrátor feladatai:

- új felhasználók (userek) rögzítése,
- meglévő felhasználók adatainak módosítása,
- felhasználók zárolása (szükség szerint),
- felhasználói jogosultságok (szerepkörök) kiosztása,
- felhasználói jogosultságok módosítása, megvonása,
- helyettesítések beállítása, eltávolítása,
- felhasználói csoportok létrehozása, módosítása, törlése (ugyanazon szerepkörök kiosztása több felhasználónak),
- üzleti napló megtekintése (a rendszerben történő változásokat lehet lekérdezni, követni).

5.2. ASP rendszerbe történő belépés, authentikáció

A Belügyminisztérium – az Igazságügyi Minisztérium és a Nemzeti Adatvédelmi és Információszabadság hatóság bevonásával – megvizsgálta azt a kérdést, hogy az elektronikus személyi igazolvány (eSZIG) felhasználása az ASP rendszerbe történő azonosításra ütközik-e valamely jogszabályba, illetve szükséges-e az önkormányzat alkalmazásában álló közszolgálati tisztviselők jogszabályi kötelezése az eSZIG kivál-tására. Ez nem ütközik jogszabályba.

Az ASP elsődleges autentikációs eszköze az eSZIG. A használatához javasolt kár-tyaolvasók hatóság által bevizsgált és elfogadott eszközök.

Az ASP eSZIG-gel történő azonosítás során személyes adathoz az ASP rendszer nem fér hozzá. Belépéskor ugyanis az e-személyi érvényességét közvetlenül a Közigazga-tási és Elektronikus Közszolgáltatások Központi Hivatalának (a továbbiakban: KEKKH) szervere ellenőrzi. A KEKKH szervere az ASP rendszernek egy ún. hash-kódot (RID) ad vissza, mely azonos okmány esetén mindig ugyanaz, de ez a kód nem fejthető vissza személyes adattá. Az ASP rendszer ehhez az anonim hash-kódhoz rendeli a felhasználót.

Az elektronikus személyigazolvánnyal történő authentikáció során a következő sza-bályzókra kell megkülönböztetett módon figyelni:

- Minden ASP rendszert használó munkatársnak rendelkeznie kell eSZIG-el.
- Az eSZIG használatához szükséges a kártyaolvasó számítógépre történő telepí-tése.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rög-zített felhasználói fiók és az eSZIG összerendelése szükséges.
- A személyi igazolvány kártyát csak a tulajdonosa használhatja, azt ASP rend-szer authentikációs folyamat céljából másnak átadni tilos.
- Az hivatal vezetőjének a Jegyzőnek gondoskodnia kell arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehető-sége biztosított legyen. Az ehhez tartozó szabályrendszer kialakítása elengedhe-tetlen.

6. Adathordozók védelmére vonatkozó eljárásrend

Általános rendelkezések mobil eszközökre vonatkozóan:

- A mobil eszközök használatát minden esetben a Hivatal vezetőjének engedélyezése kell megelőznie.
- A mobil eszközök (pl. notebook) használatára a munkaállomásokra vonatkozó szabályok érvényesek.
- Mobil eszközök igénylését a Hivatal vezetője bírálja el, engedélye alapján az IT referens adja ki, veszi vissza és tartja nyilván.

- Gondoskodni kell a mobil eszközökön tárolt adatok bizalmasságáról, azon adat csak megfelelő titkosítással tárolható.
- A mobil eszköz esetleges elvesztését lehetőség szerint azonnal, de minél előbb jelezni kell a Hivatal vezetője felé, akinek erről feljegyzést kell készítenie.

6.1. Hozzáférés adathordozókhoz

A Hivatal területén csak a táblázatban meghatározott adathordozók használata engedélyezett. Ezen adathordozókat a Hivatalból csak a Hivatal vezetőjének engedélyével lehet kivinni.

Adathordozó típus	**Szerepkör**
Hivatal által kiadott pendrive, CD, DVD	a nevére kiadottat minden felhasználó
Mentési adatokat tartalmazó adathordozók	jegyző, rendszergazda
Telepítő CD-k, DVD-k	jegyző, rendszergazda

6.2. Adathordozók törlése

Javításra átadandó készülékek esetén a rendszergazdának gondoskodnia kell arról, hogy a készüléken tárolt bizalmas adatok törlésre kerüljenek az átadás előtt.

A selejtezésre kerülő adathordozók tartalmát a rendszergazdának meg kell semmisítenie, melynek megtörténtét a *Selejtezési jegyzőkönyv*ben a leltárfelelős aláírásával igazol.

Amennyiben az eszköz többé nem kerül felhasználásra, úgy az adathordozót fizikailag kell használhatatlanná tenni (összetörni, roncsolni). Ha az adathordozó felett a hivatali ellenőrzés megszűnik, vagy újrafelhasználásra kerül kibocsátásra, előtte az eszköz tartalmát fizikai formázási mechanizmussal kell megsemmisíteni.

6.3. Adathordozók használata

Adathordozó típus	**Felhasználás Hivatal területén:**		**Tárolása**
	belül	**kívül**	
Hivatal által kiadott pendrive, CD, DVD	Csak az Hivatali munkával kapcsolatos állományok tárolására.	Jegyzői engedéllyel.	A felhasználó által elzárva.
Mentési adatokat tartalmazó adathordozók	Csak archiválási célokra használható, tárolása	Jegyzői engedéllyel.	Zárt páncélszekrényben.
Telepítő CD-k, DVD-k	Csak a Hivatal gépein használhatóak a licence-k keretein belül	Jegyzői engedéllyel.	Zárt páncélszekrényben.

6. Külső elektronikus információs rendszerek használata

A Hivatal információs rendszereihez távoli hozzáférést a következő személyeknek biztosít:

Elérhető rendszer	szerepkör
-	-

7. Nyilvánosan elérhető tartalom

Az interneten és más nyilvános csatornákon történő, a Hivatallal kapcsolatos információk közzétételére vonatkozó jogosultságok:

Tevékenység	Szerepkör
publikálható adatok engedélyezése	jegyző
adatok publikálása	IT referens

Kelt: Kocsord, 2020. április 01.

Dr. Gellért-Kovács Adrienn
jegyző