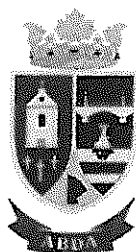


ABDAI KÖZÖS ÖNKORMÁNYZATI HIVATAL

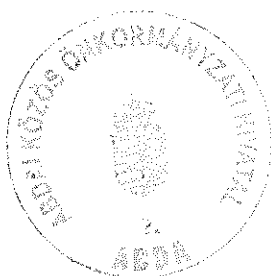
ENGEDÉLYEZÉSI ÉS JOGOSULTSÁGI SZABÁLYZAT

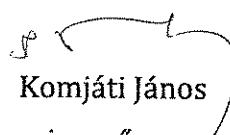


Verziószám: 1.0

Iktatási szám:

Dátum: 2018. 01. 02.




Komjáti János
jegyző

Tartalomjegyzék

1. Általános rendelkezések.....	4
1.1. A szabályzat célja	4
1.2. A szabályzat hatálya.....	4
1.3. Az engedélyezés és jogosultság céljai	4
1.4. Definíciók.....	4
1.5. Felelősségek	4
1.5.1 A Hivatal vezetése	4
1.5.2 Az IBF.....	4
1.5.3 A munkatársak.....	4
2. A fiókkezelés szabályozása.....	5
2.1. A fiókkezeléssel kapcsolatos elvárások	5
2.2. A fiók elnevezési szabályai (névkonvenció)	5
2.3. Fiók létrehozása, módosítása, törlése	5
3. A jogosultságok szabályozása.....	6
3.1. A jogosultságokkal kapcsolatos elvárások.....	6
3.2. A jogosultságok elnevezési szabályai (névkonvenció).....	6
3.3. A szerepkörök és jogosultságok megváltoztatása.....	6
3.4. A szerepkörök és jogosultságok ellenőrzése	6
4. Hozzáférés-védelem.....	7
4.1. Felhasználó kezelés.....	7
4.2. Általános elvárások.....	7
4.2.1 Jogosultságok igénylése	8
4.2.2 Jogosultsági igény jóváhagyása, továbbítása.....	8
4.2.3 Felhasználó felvétele	8
4.2.4 Jogosultságok módosítása.....	9
4.2.5 Felhasználó kilépése.....	9
4.3. Kiemelt felhasználói jogosultság kezelése.....	9
4.3.6 Jogosultság igénylése	9
4.3.7 Kiemelt jogosultság használata.....	10
4.3.8 Jogosultság megvonása	10
4.4. Technikai azonosítók kezelése	10
4.5. Felhasználói azonosító és jogosultságok használata.....	10
4.5.9 Jelszókezelés szabályai.....	10
4.5.10 Kiemelt felhasználói és technikai azonosítók jelszavai.....	11
4.5.11 Külső harmadik fél hozzáférés védelme.....	12
4.5.12 Tanúsítványok használata.....	12

4.6. Jogosultságok nyilvántartása	12
4.7. A jogosultságok felülvizsgálatának rendje	12
5. Egyéb rendelkezések.....	13
5.1. Fiókok és jogosultságok dokumentálása.....	13
5.2. Egyéb biztonsági követelmények, ajánlások	13
5.3. Általános korlátozások	13

1. Általános rendelkezések

1.1. A szabályzat célja

Jelen szabályzat rendelkezik a Abdai Közös Önkormányzati Hivatal (továbbiakban: Hivatal) információs rendszereinek a szerepkörök és jogosultságok tekintetében támasztott elvárásairól, melyeket rendszerteknikailag valósítottunk meg.

1.2. A szabályzat hatálya

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

1.3. Az engedélyezés és jogosultság céljai

- a) a Hivatalnál csak az arra jogosult személyek rendelkeznek hozzáféréssel a rendszerekhez és az információkhoz;
- b) a vezetők és az alkalmazottak ismerik a feladatokat és a szükséges jogokat;
- c) valamennyi felhasználó személyre szóló felhasználói jogosultsággal rendelkezik;
- d) kerüljük az ellentmondó vagy egymást kioltó jogosultságokat, szerepköröket;
- e) a jogosultságok igénylése, engedélyezése, visszavonása dokumentált;

1.4. Definíciók

1. *felhasználói fiókok (user accountok)*: a felhasználói fiókok a hálózatokon vagy alkalmazásokon belül a felhasználó egyértelmű beazonosítására szolgál. Egy felhasználói fiók több szerepkörhöz is tartozhat.

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 mindenkorai felhasználó interaktív tevékenységét, hanem pl. az IT-rendszerek közötti adatcseréhez szükségesek

1.5. Felelőségek

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 IBF

- a) felelős a jogosultságok kialakításáért és nyilvántartásáért
- 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 felhasználó önálló, személyre szóló fiókot kap, amely egyértelműen beazonosítható
- c) tiltjuk a más személyek felé, ill. más személyek által történő továbbadást vagy felhasználást
- d) a felhasználói fiókokat egységes névkonvenció szerint hozzuk létre
- 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 létesítünk, elkülönítve a normális jogosultságot igénylő feladatokhoz használt fióktól
- f) minden szolgáltatás fiókot (service accountot) felelőshöz rendelünk, aki felelős a szolgáltatás fiók aktualizálásáért és törléséért, jelszavainak rendszeres megváltoztatásáért
- g) biztosítjuk, hogy csak feljogosított dolgozók ismerjék a szolgáltatás fiókok (service accountok) jelszavát.
- h) valamennyi felhasználói fiókot és annak módosítását dokumentáljuk. Ennek kapcsán figyelembe vesszük az ellenőrzési követelményeket is.

2.2. A fiókok elnevezési szabályai (névkonvenció)

A felhasználói fiókokat egyértelműen adjuk ki. Amennyiben technikailag lehetséges, úgy már a felhasználói elnevezésből világosan felismerhetőek, hogy az adott fiók rendelkezik-e privilegizált jogokkal (pl. „gipsz.j_admin”), továbbá az elnevezésből levezethető maga a felhasználó (pl. „gipsz.j”) vagy szolgáltatás fiók esetén a feladatkör (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. Ez az engedélyezési folyamat mindenkor nyomon követhetően dokumentált oly módon, hogy vizsgálat esetén rövid időn belül és hiánytalanul igazolásokat lehet felmutatni.

A felhasználói fiókok igénylését és engedélyezését a területen belül két különböző személy hajtja végre. A felhasználói fiókok kezelése a rendszergazdák felelősségi köréhez tartozik.

Felhasználói fiókot csak olyan személyek részére adunk ki, akik elfogadják a Hivatal információbiztonsági szabályait. Az elfogadást írásos úton adjuk meg és az nyomon követően dokumentált, amely a szerződés mellékletét képezheti. Ez különösen a külső szolgáltatókra érvényes.

A már nem szükséges fiókokat inaktívvá változtatjuk és három hónap elteltével töröljük. 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 csak szerepkörökön keresztül adjuk ki és kerüljük az egyéni joghozzárendeléseket. Amennyiben ez nem lehetséges, úgy az eltéréseket külön dokumentáljuk és az alkalmazásukat, valamint szükségességüket rendszeresen ellenőrizzük.
- 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 történik, azaz a szakterület részéről szakmailag meghatározott szétválasztásoknak a kiadott és rendszertechnikailag hozzárendelt jogokban tükröződnek vissza.
- d) kerüljük az egymásnak ellentmondó, ill. egymást kioltó jogosultságokkal rendelkező szerepköröket. Az eltéréseket dokumentáljuk, indokoljuk és azokat kivételként engedélyezzük.

3.2. A jogosultságok elnevezési szabályai (névkonvenció)

Valamennyi meghatározott szerepkört és jogosultságot egységes elnevezési szabály szerint névvel látjuk el, 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 hajtjuk végre. Ennek során az alábbi folyamatokat vesszük figyelembe:

- 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 személyzeti osztály és a szakterületek funkciójuk keretében valamennyi személyi változást és a jogosultságok ebből eredő változásait a felelős adminisztrátorok felé a jogosultságok minél korábbi illesztése érdekében közvetlenül lejelenti.

Ennek során főként azt biztosítjuk, 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 felülvizsgálunk. Az osztályvezetők meggyőződnek a meghonosított szerepkörök megfelelőségéről, a szerepkörök hozzárendelésének megfelelőségéről és esetleg a felhasználók járulékos egyéni jogosultságainak helyességéről. Az eltéréseket jelentjük az IBF-nek.

4. Hozzáférés-védelem

A Hivatal kizárólag nyilvánosan hozzáférhető adatokat tartalmazó elektronikus információs rendszereinek elérése során felhasználói szintű hozzáférés-védelem használata nem elvárás.

A nem kizárólag nyilvános adatokat tartalmazó elektronikus információs rendszereknek rendelkeznek a felhasználók azonosítását, hitelesítését megbízható módon lehetővé tevő hozzáférés-védelmi rendszerrel. Az elektronikus információs rendszer hozzáférés-védelmi rendszere biztosítja, hogy azokat a funkciókat, amelyek alkalmasak a kezelt adatok valamely védendő biztonsági kritériumának (bizalmasságának, sértetlenségének, rendelkezésre állásának) kompromittálására azonosítás és hitelesítés nélkül ne lehessen használni.

A rendszerek autentikációjának beállítása során törekszünk a felhasználói azonosítók egységes, központi felületen történő kezelésére. Azon rendszerek esetén, amelyek lehetővé teszik, hogy a felhasználók azonosítása, hitelesítése központi címtárban tárolt adatok alapján történjen, ott lehetőség szerint kerüljük a lokális felhasználók használatát, ettől csak üzemeltetési szempontból indokolt esetben, a jegyző jóváhagyásával lehet eltérni.

A rendszerekben lehetőség szerint személyhez rendelt azonosítókat használunk, ettől eltérni – azaz felhasználói csoport által közösen használt azonosító használatára – csak a jegyző írásbeli engedélye esetén szabad, mely engedély indokolja, hogy milyen technikai, ügyvitelszervezési vagy egyéb oka van annak, hogy személyhez rendelt azonosítók nem használhatók.

A Hivatal informatikai hálózatában csak a jegyző által jóváhagyott informatikai eszköz telepíthető. A hivatal felhasználója alapértelmezetten nem lehet jogosult az informatikai eszközön kiemelt felhasználói jog használatára, mely szabály alól jegyzői engedéllyel el lehet térni, azonban ilyen esetekben külön nyilvántartással rendelkezik a Hivatalnak ezen többletjogosultsággal rendelkező felhasználókról, továbbá indokolni szükséges a többletjogosultság használatát.

4.1. Felhasználó kezelés

A jegyző feladata és felelőssége, hogy a felhasználók felvétele, kilépése, áthelyezése, az esetleges átszervezések, illetve a felhasználók feladatkörének változtatása kapcsán olyan munkarendet alakítson ki, ami biztosítja, hogy a felhasználók az informatikai rendszerekhez mindenkor csak a feladatkörük ellátásához szükséges jogosultságokkal férjenek hozzá. E követelmények teljesítése érdekében centralizált jogosultságkezelési és nyilvántartási, a jogosultságkezelés teljes életciklusára kiterjedő folyamatot alakít ki és működtet a Hivatalban.

4.2. Általános elvárások

- új felhasználó felvétele esetén csak a feladatköre ellátásához szükséges informatikai rendszerekhez és csak a szükséges jogosultságok erejéig kapjon hozzáférést;
- a hozzáférés csak akkor bocsátható a felhasználó rendelkezésére, ha minden feltételt biztosított ahhoz, hogy azt a felhasználó biztonságosan, jelen szabályzatban leírtakkal összhangban tudja használni;
- áthelyezés, átszervezés, illetve a felhasználó feladatkörének változása esetén, a már nem szükséges hozzáférések, jogosultságok kerüljenek visszavonásra;
- kilépés, tartós távollét, a felhasználó jogviszonyának megszűnése, vagy felfüggesztése esetén a felhasználó hozzáférési jogosultságai visszavonásra, tiltásra kerüljenek.

A fenti általános követelmények egyformán érvényesek a Hivatal saját informatikai rendszerein, a külső szolgáltatótól igénybe vett rendszerek esetén, illetve minden olyan internetes szolgáltatás esetén, ahová a felhasználók a Hivatal tevékenységével kapcsolatos feladatokhoz regisztrált hozzáférést használnak.

A jegyző felelőssége, hogy a fenti követelmények maradéktalan teljesítése érdekében minden érintett informatikai rendszer esetén az adott rendszer üzemeltetési feladatait ellátó személy értesítést kapjon a felhasználó hozzáférési jogosultságainak szükséges módosításáról.

4.2.1 Jogosultságok igénylése

A Hivatal informatikai rendszereihez jogosultságokat a Hivatal munkatársai a jegyzőtől igényelhetnek, írásban vagy szóban. A hozzáférési jogosultságot igényelni a Hivatal belső informatikai infrastruktúráján futó alapszolgáltatások eléréséhez és használatához, belső alkalmazások, külső szolgáltató által biztosított alkalmazások és szolgáltatások, illetve központi szolgáltatások igénybevételéhez lehetséges.

Új munkatárs munkába lépésekor a jegyző határozza meg a munkatárs munkakörének megfelelő rendszerhozzáféréseket, és a rendszerekben beállítandó jogosultságokat.

4.2.2 Jogosultsági igény jóváhagyása, továbbítása

A jegyző egyszemélyben felelős az igényelt hozzáférési jogosultságok jóváhagyásáról dönteni. A jegyzőnek a döntésének megfelelően írásban szükséges rögzítenie a jóváhagyott jogosultságokat, és továbbítani a rendszergazdának, illetve az adott rendszer üzemeltetőjének (amennyiben nem a rendszergazda látja el az adott rendszer rendszerüzemeltetési feladatait) a kért és beállítandó jogosultságokat.

A jogosultsági igények továbbítása email-en vagy papír alapon is történhet. Az igénynek minimálisan tartalmazniuk kell, hogy:

- mely felhasználóhoz kapcsolódóan történt az igénybejelentés;
- mely rendszerhez kapcsolódik az igény;
- milyen rendszeren belüli jogosultság beállítása szükséges

A fenti adatokon felül az adott rendszer üzemeltetője (pl. központi rendszerek esetében) egyéb adatok megadását illetve egyedi jogosultság bejelentő formanyomtatvány használatát is megkövetelheti, melynek megfelelően szükséges a jegyzőnek az igénylést végrehajtani.

Érvénytelen az igénylés, ha nem tartalmaz minden olyan információt, mely alapján az üzemeltető be tudja állítani a kérvény alapján az igényelt jogosultságokat, továbbá, ha az igénylés e-mail esetén nem a jegyző e-mail címéről érkezett, papír alapú igény esetén nem tartalmazza a jegyző aláírását.

A jegyző felelőssége a jóváhagyott és beállításra továbbított jogosultsági igények papír alapon történő megőrzése (e-mailen történt igénylés esetén az e-mail nyomtatásával) az igényléstől számított 3 évig. A jegyző feladata, hogy minden jóváhagyott jogosultsági igényről írásban tájékoztassa a Hivatal rendszergazdáját.

Az érintett informatikai rendszerek üzemeltetési feladatait ellátók kötelesek a jegyző által jóváhagyott igények alapján végrehajtani a jogosultsági igények beállítását az érintett rendszerekben.

4.2.3 Felhasználó felvétele

A Hivatal üzemeltetési hatáskörében lévő rendszerek esetében a jogosultságot beállító rendszergazdának az alábbi szabályok szerint eljárnia:

- új felhasználó esetében az érintett rendszer(ek)ben létrehozuk a hozzáféréshez szükséges azonosítókat, üzemeltetőnek törekszünk a felhasználói azonosító egységes képzési szabályára;
- az érintett rendszer(ek)ben az létrehozuk a használatához szükséges objektumokat (pl. postafiók, saját mappa a fájlserveren)

- az érintett rendszer(ek)ben a felhasználót az igénylésben meghatározottak szerint hozzáférési jogosultsággal ruházza fel
- a rendszergazda feladata gondoskodni a kapcsolódó nyilvántartások (pl. jogosultság, licenc) frissítéséről.
- a felhasználó kezdeti jelszavát a rendszergazda köteles megválasztani, a rendszergazda feladata felhívni a felhasználó figyelmét, hogy az első bejelentkezés alkalmával változtassa azt meg
- a rendszergazdának a jelszót a felhasználónak úgy adjuk át, hogy annak bizalmassága ne sérüljön

Nem hivatali hatáskörben üzemeltetett rendszerek esetében a rendszer üzemeltetését végző fél feladata a belső eljárásrendjének megfelelően regisztrálni az érintett rendszerben az igénylésben szereplő jogosultságokat.

4.2.4 Jogosultságok módosítása

Hozzáférési jogosultságok módosítása (új jog kiadása, meglévő jog elvétele) a 4 és 4-as pontban leírtak szerint történik.

4.2.5 Felhasználó kilépése

A jogviszony megszűnéskor jegyzői felelőssége gondoskodni arról, hogy a kilépő munkatárs esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzze (pl. hozzáférések megszüntetése, jogosultságok visszavonása).

A távozó munkavállaló jogosultságainak visszavonását a jegyző írásban (e-mailen, papíron) kezdeményezi, minden olyan informatikai rendszerre kiterjedően (helyi rendszerek, külső harmadik félnél üzemeltetett rendszerek esetében is), melyhez hozzáférési jogosultsággal rendelkezett a kilépő személy. A kilépéskor, a Hivatal által üzemeltetett rendszerekben, a jogosultságot visszavonó rendszergazdának írásban igazolja, hogy a kilépő munkatárs hozzáféréseit minden általa üzemeltetett rendszerben megszüntette, illetve ha az ő közreműködésével történt a külső rendszerekben lévő jogosultságok visszavonása úgy ezen rendszerekben végrehajtott változásokról is értesíti a jegyzőt. Ha nincs lehetőség a jogosultságok visszavonására, akkor a jelszó megváltoztatásával akadályozzuk meg az azonosító használatát. Ilyen esetben a megváltoztatott jelszót a jegyző zárt borítékban elzárt helyen tárolja.

Abban az esetben, ha a felhasználó jogviszonya, illetve a kapott hozzáférés oka megszűnik, akkor a Hivatal fenntartja a jogot, hogy a felhasználó által kezelt adatokat a jegyző engedélyével mások számára - pl. a munkahelyi vezető vagy az általa kijelölt munkatárs számára - hozzáférhetővé tegye, vagy archiválja. A munkaviszony megszűnése előtt a felhasználónak kötelessége felhasználói azonosítóját átadni, személyes használatú adatait törölni. A felhasználó a Hivatal tulajdonát képező adatokat kilépéskor nem semmisíthet meg!

4.3. Kiemelt felhasználói jogosultság kezelése

4.3.6 Jogosultság igénylése

A Hivatal felhasználói számára az informatikai rendszerekhez kiemelt felhasználó jogosultság a jegyző írásos beleegyezésével adható ki. A jogosultságigénylés a 4.2.1 fejezet előírásai szerint kell végrehajtani. A kiemelt felhasználói jogosultságokról a rendszergazda a normál felhasználói jogosultságokhoz hasonlóan nyilvántartást vezet.

4.3.7 Kiemelt jogosultság használata

Kiemelt felhasználói jogot biztosító felhasználói azonosítóval kizárólag üzemeltetési feladatok, illetve olyan ügyviteli tevékenységek (pl. kiemelt felhasználói jogosultság szükséges ügyviteli alkalmazás használatához) láthatók el, melyek megkövetelik ezen azonosító használatát.

4.3.8 Jogosultság megvonása

A jegyző kezdeményezheti a kiemelt felhasználói jogosultság azonnali hatállyal történő megvonását. A jogosult munkakörének megváltozása, kilépése azonnal a jog megszüntetését vonja maga után. A kiemelt felhasználói jogok visszavonásának módja:

- azon rendszereken, ahol a kiemelt felhasználói jog nem köthető személyhez, ott a kiemelt felhasználói jelszót haladéktalanul megváltoztatjuk;
- azon rendszerek esetén, ahol az adminisztrátori szerep a felhasználói azonosítóhoz rendelt, ott a felhasználó és a szerep kapcsolatát megszüntetjük.

4.4. Technikai azonosítók kezelése

A technikai azonosítók igénylése és kezelése a kiemelt felhasználói azonosítókéval megegyező módon történik. A hozzáférési jogosultságokról vezetett nyilvántartásnak tartalmazza a technikai azonosítókat is, feltüntetve a technikai azonosító használatának célját, valamint a technikai azonosító felelőseit.

4.5. Felhasználói azonosító és jogosultságok használata

Minden felhasználó felelős a feladatköre ellátásához kapott informatikai hozzáférésekhez tartozó azonosító és hitelesítő adatok védelméért, biztonságos használatáért. Egyes rendszerek az azonosításhoz szükséges felhasználói név és a hitelesítéshez szükséges jelszó mellett megkövetelhetik további azonosító, illetve hitelesítő eszközök – pl. tokenek, chip kártyák, tanúsítványok – használatát. Ezek szintén fokozott körültekintéssel, a kapcsolódó szabályok megismerése és betartása mellett kezelendők.

A hitelesítő adatok (például a felhasználói jelszó) védelme a felhasználó kötelessége és felelőssége. A jelszókezeléssel kapcsolatos mulasztásért a felhasználó felel.

A több felhasználó által közösen használt azonosítókhoz tartozó jelszót haladéktalanul megváltoztatjuk, ha a jelszót ismerők bármelyikének a jogosultsága megszűnik (pl. áthelyezés, munkaviszony megszűnése).

Technikai azonosítót a felhasználók a napi feladataik elvégzéséhez nem használhatnak. A technikai azonosítók jelszavát haladéktalanul megváltoztatjuk, ha az azt ismerő munkatársak valamelyikének a Hivatallal való kapcsolata (pl. munkaviszony, szerződés) megszűnik.

4.5.9 Jelszókezelés szabályai

A felhasználó számára annak érdekében, hogy csökkentse a részére átadott felhasználói azonosítókkal esetlegesen elkövethető visszaéléseket, az alábbi irányelvek követése javasolt:

- Jelszókezeléssel kapcsolatos irányelvek
 - A jelszavakat tilos jogosulatlanok számára hozzáférhető helyen leírva tárolni, a leírással szemben az emlékezetben tartás preferált!
 - A jelszót csak és kizárólag az alkalmazás igénybevételét lehetővé tevő bejelentkezési ablakba szabad begépelni! Ha a felhasználó a bejelentkezési ablaknál bármilyen rendellenességet tapasztal, ne gépelje be a jelszavát, azonnal értesítse az informatikai rendszer üzemeltetésével megbízott kollégát.
 - A személyhez rendelt jelszavakat másokkal megosztani TILOS! A felhasználó, a részére kiosztott jogosultsággal elkövetett visszaélésekért, biztonságsértésért - akár

az a személyhez rendelt felhasználói név/jelszó pár átadásának vagy eltulajdonításának következménye - személyesen, a tényleges károkozóval egyetemlegesen felel!

- A felhasználó a részére kiadott felhasználói azonosítókat és jelszavakat csak azokon az eszközökön használja, melyek hozzáférésehez kapta. Nem célszerű azt más, esetleg szabadon hozzáférhető, rendszereken használni.
- A jelszavakat javasolt rendszeresen, pl. 90 naponta megváltoztatni, ez alól kivétel az az eset, amikor a jelszó illetéktelenek birtokába jut vagy ennek veszélye áll fenn, mert ekkor azonnali jelszóváltoztatás kötelező!
- Jelszó kompromittálódása esetén azt azonnal megváltoztatjuk, valamint a biztonsági események jelentésénél leírtak szerint jelezzük az informatikai rendszer üzemeltetésével megbízott felé és értesítjük a felhasználó közvetlen felettesét.
- A biztonságos jelszó nem azt jelenti, hogy a felhasználó kitalál egy számára kedves szót, amit jelszónak tekint, hanem olyan szó vagy betűsorozat alkalmazása, mely mások által nehezen kitalálható és visszafejthető, a felhasználó személyéhez a lehető legkisebb mértékben köthető. Ellenkező esetben a támadó – aki ismeretekkel rendelkezik a felhasználóról és a környezetéről – képes szótárat készíteni a lehetséges szavakból és visszafejteni a felhasználói jelszavakat. Annak érdekében, hogy e visszaélések ne történjenek meg, az alábbi jelszóválasztási vezérelveket is javasolt figyelembe venni:
 - a jelszó hossza legalább 8 karakter hosszú legyen, vagy ha ezt az adott informatikai rendszer nem támogatja, akkor a rendszer által használható maximális hosszúság;
 - a jelszó SOHASE legyen személyes, személyhez köthető szó; mint pl.: a kedvenc autó típusa, az üzőtt sportág neve, születési idő, telefonszám, a kedvenc háziállat, gyerekek vagy házastárs neve, kedvenc étel vagy könyv címe;
 - SOHA sem lehet a jelszó azonos a felhasználói névvel vagy a felhasználó valódi nevével, illetve a felhasználói név nem lehet része a jelszónak;
 - a jelszavakat TILOS szótárakból választani, mert a legtöbb jelszótörő program szótárat használ a próbálgatáskor;
 - a jelszavak megválasztásakor vegyesen használjon a felhasználó betűket (kis- és nagybetű vegyesen: a-z, A-Z), számokat, egyéb írásjeleket (*@&(_+...) és üres karaktert.
 - a jelszóban nem fordulhat elő ugyanaz a karakter egymás mellett álló pozícióban kettőnél többször,
 - a billentyűzeten egymás mellett álló karakterek sorozata sem elfogadható,
 - a jelszó megválasztásakor törekszünk arra, hogy könnyen gépelhető és megjegyezhető legyen (pl. „Boci boci tarka, Se füle se farka” alapján a jelszó képzési szabálya lehet: minden kezdőbetű az adott szó hosszával kiegészítve, „B4b4t5,S2f4s2f5”).
- Tekintettel arra, hogy a felhasználó jelszava a biztonság szempontjából kiemelten védendő, ezért egyes informatikai rendszerek adott számú sikertelen bejelentkezési kísérletet esetén automatikusan kitiltják az adott felhasználót, így védve a felhasználót attól, hogy a támadó jogosulatlanul a felhasználó nevében kárt okozzon. Ilyen esetben az adott rendszer üzemeltetési feladataiért felelős munkatársat kell keresni új jelszó igénylése miatt.

4.5.10 Kiemelt felhasználói és technikai azonosítók jelszavai

A rendszerek kiemelt felhasználói azonosítói és a technikai azonosítók esetén a felhasználói jelszókezelés szabályain túl a jelszó megőrzését, hozzáférhetőségét a Hivatal rendszergazdája biztosítja olyan módon, hogy a jelszavakhoz illetéktelenek ne férjenek hozzá. A megőrzés, illetve

hozzáférhetővé tétel módját a jegyző határozza meg, és bármikor ellenőrizheti (pl. a jelszó páncélszekrényben zárt borítékban vagy védett fájlban való tárolásával).

A kiemelt felhasználói és technikai jelszavak esetén a jelszó hosszának minimálisan 12 karakteresnek kell lennie.

4.5.11 Külső harmadik fél hozzáférés védelme

A külső felek hozzáféréseinek biztonságát szerződés szintjén is meghatározzuk és ennek kapcsán kitérünk az adminisztrációhoz és az adatok bizalmas kezeléséhez kapcsolódó követelményekre is. Kiszervezés esetén a felek között megkötött szerződésben kitérünk a kockázatok és az információs rendszerekhez és hálózatokhoz kapcsolódó biztonsági ellenőrzések és eljárások kérdésére.

4.5.12 Tanúsítványok használata

A Hivatal elektronikus információs rendszerei külső felhasználók hitelesítéséhez csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadja el.

A szakrendszerekhez használt külső tanúsítványokat a jegyző feladata igényelni a Hivatal rendszergazdájának támogatása mellett. A Hivatal rendszergazdájának feladata a Hivatal által használt tanúsítványokról naprakész nyilvántartást vezetni mely nyilvántartásnak tartalmazza a tanúsítványhoz kapcsolódó rendszert és a tanúsítvány lejáratát. A rendszergazda feladata ezen tanúsítványok lejáratát megelőző egy hónappal kezdeményezni a jegyzőnél az új tanúsítvány beszerzését.

A hitelesítés szolgáltatótól beszerzett tanúsítványok privát kulcsáról a Hivatal rendszergazdájának másolatot készít és a jegyző által meghatározott helyen kell tárolja.

4.6. Jogosultságok nyilvántartása

A Hivatal centralizált jogosultságkezelési és –nyilvántartási rendszert működtet. Ennek keretében minden használt elektronikus információs sziszterről, beleértve –

- a belső hálózatában üzemelő, belső üzemeltetésű,
- a belső hálózatában üzemelő, harmadik fél által üzemeltetett, valamint
- a belső hálózatán kívül harmadik fél által üzemeltetett

rendszert – egységes jogosultság nyilvántartást vezet. A jogosultság nyilvántartás naprakészen tartása és annak biztonságos tárolása a jegyző felelőssége.

A nyilvántartásnak tartalmazza az adott rendszerben aktuálisan létező felhasználói azonosítókat, az azonosítókat birtokló, használó munkatárs(ak) nevét, valamint a rendszerben beállított jogosultságainak felsorolását, a kiemelt és technikai azonosítók mellett.

Az aktuális jogosultság nyilvántartás elkészítése, karbantartása a Hivatal rendszergazdájának a feladata.

4.7. A jogosultságok felülvizsgálatának rendje

A jegyző bármikor jogosult a fenti követelmények teljesülését ellenőrizni, vagy ilyen jellegű ellenőrzést elrendelni, de legalább éves rendszerességgel szükséges végrehajtani a jogosultságok felülvizsgálatát.

5. Egyéb rendelkezések

5.1. Fiókok és jogosultságok dokumentálása

A rendszergazdák 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)

5.2. Egyéb biztonsági követelmények, ajánlások

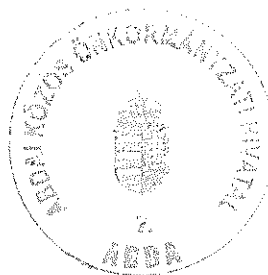
- a) az információbiztonság garantálása céljából valamennyi hozzáférési kísérletet naplózzuk
- b) többszöri sikertelen bejelentkezési kísérletet követően az érintett fiókot automatikusan zároljuk (a zárolás feloldásának módja lehet automatikus, vagy manuális is)
- c) az inaktív munkameneteket meghatározott idő után zároljuk, vagy megszakítjuk
- d) minden szolgáltatás esetében törekszünk a központosított hitelesítésre (pl. LDAP)
- e) törekedünk a 4 szem-elvre: a jogosultságok engedélyezése és azok rendszertехnikai felvétele legalább +1 fő ellenőrzése mellett történik

5.3. 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)

Abda, 2018. január 02.



Komjáti János
jegyző

Hozzáférések nyilvántartása űrlap

[illegible]

Hozzáférési jogok igénylése űrlap

Jogosultságigénylő adatai

Igénylő neve:
Szervezeti egység:
Telefon:
E-mail:

Igényelt művelet

Jogosultság kezdete: Jogosultság vége:.....
Új jogosultság ☐ Jogosultság törlése ☐ Jogosultság módosítása ☐

Jogosultság

Indoklás

A jogosultságigényléshez kapcsolódó feladatellátás megnevezése:

.....
.....

Kelt: igénylő aláírása

Munkahelyi vezető jóváhagyás

Vezető:

Beosztása:

Kelt: vezető aláírása

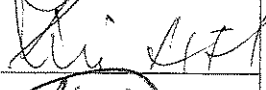
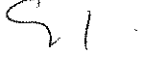
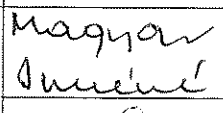
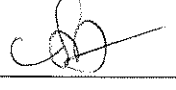
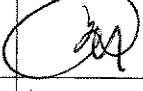
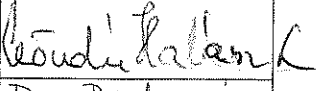
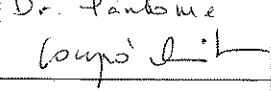
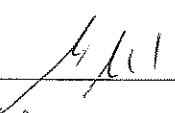
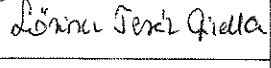
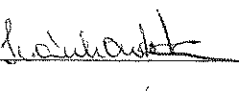
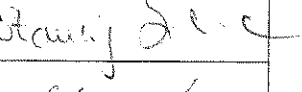
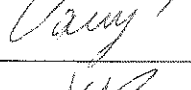
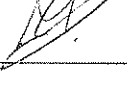
Jogosultságot beállító aláírása

IT felelős:

Kelt: IT felelős aláírása

Megismerési nyilatkozat

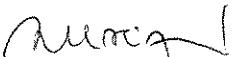
az Abdai Közös Önkormányzati Hivatal Engedélyezési és Jogosultsági Szabályzatához

Név	Feladat, hatáskör	Dátum	Aláírás
Szabó Zsolt	polgármester	2018.01.02	
Rácz Róbert	polgármester	2018.01.02	
Németh Tamás	polgármester	2018.01.02	
dr. Dukkon Eszter	aljegyző	2018.01.02	
Szémann-né Hegedüs Edit	gazdálkodási ea.	2018.01.02	
Magyar Imréné	gazd. csoportvezető	2018.01.02	
Asztalos-Rácz Szilvia	gazd. ea.	2018.01.02	
Rigóné Finta Anikó	adóügyi ea.	2018.01.02	
Saru Dániel	közbizt./településüzem. ea.	2018.01.02	
Csöndesné Halász Erika	igazgatási ea.	2018.01.02	
Dr. Pásztorné Csapó Anita	igazgatási ea.	2018.01.02	
Ivánkovits Zsolt Istvánné	igazgatási ea.	2018.01.02	
Lőrincz Teréz Gizella	gazd.ea.	2018.01.02	
Ivánkovits Vivien	igazgatási ea.	2018.01.02	
Stancig Szilvia	ügykezelő	2018.01.02	
Varju Gyula Csabáné	gazd.ea.	2018.01.02	
Marx-Morvay Katalin	polgármesteri referens	2018.01.02	

[illegible]

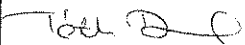
Megismerési nyilatkozat

az Abdai Közös Önkormányzati Hivatal Engedélyezési és
Jogosultsági Szabályzatához

Név	Feladat, hatáskör	Dátum	Aláírás
Pollreiszné Foki Anikó	gazd.ea.	2018.03.01.	

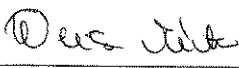
Megismerési nyilatkozat

az Abdai Közös Önkormányzati Hivatal Engedélyezési és
Jogosultsági Szabályzatához

Név	Feladat, hataskör	Dátum	Aláírás
Tóth Dóra	gazd. ca.	2018.04.16	

Megismerési nyilatkozat

az Abdai Közös Önkormányzati Hivatal Engedélyezési és
Jogosultsági Szabályzatához

Név	Feladat, hatáskör	Dátum	Aláírás
Weisz Márta	igazgatási ea.	2018.11..16.	

Megismerési nyilatkozat

az Abdai Közös Önkormányzati Hivatal Engedélyezési és
Jogosultsági Szabályzatához

Név	Feladat, hatáskör	Dátum	Aláírás
Burnóczki Renáta	pénzügyi/számviteli üi.	2019.07.01.	Burnóczki Renáta