

**A Bástya Millenium Zrt.  
Mentési Szabályzata  
2023. 01. 01.**

Óry Edit  
Igazgatósági tag

Bástya Millenium Zrt.

## Tartalomjegyzék

A szabályzat célja .....	3
A szabályzat hatálya .....	3
Fogalmak .....	3
A szabályzathoz kapcsolódó szerepkörök .....	4
A mentési és visszaállítási rendszerrel szemben támasztott követelmények .....	4
Mentendő adatok köre .....	5
Mentési irányelvek .....	5
Az operációsrendszerek mentése .....	6
Az alkalmazás állományok mentése .....	6
Az adatbázisok mentése .....	6
Fájlmentés .....	6
A mentett adatok és mentési médiák kezelése .....	6
A mentett adatok logikai védelme .....	6
A mentett adatok fizikai védelme .....	7
A mentési médiák kezelése .....	7
A mentési infrastruktúra leírása .....	7
A mentési logika leírása .....	7
Adatvesztési ablakok: .....	8
A visszaállítás szabályozása .....	8
Egyes állományok visszaállítása .....	8
Teljes rendszer visszaállítása .....	9
A mentő szerver mentése és visszaállítása .....	9
A szerepkörök feladatai a mentés-visszaállítás során .....	9
Mentési adminisztrátor .....	9
Alkalmazás rendszergazda .....	9
Üzemeltetési vezető .....	10
Felhasználó .....	10
Az utasítás felülvizsgálata és a szabályoktól való átmeneti eltérés dokumentálása .....	10

## A szabályzat célja

A szabályzat célja, hogy meghatározza a Bástya Millenium Zrt. informatikai rendszereinek (rendszoftverek, alkalmazások, adatbázisok stb.) biztonsági mentéssel és visszaállítással kapcsolatos egységes követelményeit, feladatköreit, valamint a mentési eljárást.

## A szabályzat hatálya

A szabályzat személyi hatálya kiterjed a Bástya Millenium Zrt. informatikai rendszereire, dolgozóira, valamint az informatikai rendszerrel kapcsolatba kerülő külső szolgáltatókra egyaránt.

A szabályzat tárgyi hatálya kiterjed a Bástya Millenium Zrt. saját informatikai rendszereire, illetve azokra a rendszerekre, melyek üzemeltetéséért külső szolgáltatók felelősek.

## Fogalmak

- **Adatbázis:** Adatok és a köztük lévő kapcsolatok rendezett formában történő kezelésére, tárolására szolgáló alkalmazás.
- **Adatgazda:** Az a munkahelyi vezető, aki felelős a vezetése alatt álló területen keletkező adatok, információk tekintetében a bizalmassági, sértetlenségi, rendelkezésre-állási, jogszabályi és egyéb külső, belső követelmények teljesítéséért.
- **Adatmentés:** Elektronikusan tárolt adatokról biztonsági másolat készítése.
- **Agent („ügynök”):** Olyan kisméretű alkalmazás, mely a mentendő számítógépen fut, és képes a mentő szerveren beállított szabályokat („policy”) érvényre juttatni a mentendő számítógépről történő adatmentés során. Segítségével adatok hálózaton keresztül történő mentése is megvalósítható.
- **Archiválás:** Mentett adatok hosszabb időre történő tárolása későbbi visszakeresés céljából.
- **Archiválandó adat:** Azok az adatok, amiket az adatgazda archiválásra jelölt ki.
- **Bar Code:** Szalagos mentési médiák egyértelmű azonosítására szolgáló vonalkódos azonosító.
- **Checksum:** Ellenőrzőösszeg. Egy adott adatsor elemeinek összeadásával képzett összeg, amelynek segítségével az adatsorban bekövetkező változások és sérülések felismerhetők.
- **CRC:** „Cyclic redundancy check” olyan, a digitális kommunikációban alkalmazott egyik leggyakoribb hibaellenőrzési eljárás, amely kis számítási kapacitás és többlet mellett biztosít igen jó módszert az átvitel során esetlegesen keletkező hibák felderítésére.
- **Differenciális mentés:** az utolsó teljes körű mentés óta bekövetkezett változások rögzítése.
- **Disaster Recovery** (katasztrófát követő helyreállítás): A rendszer helyreállítása teljes körű mentésből és előre elkészített visszaállító médiák alkalmazásával, az eredetivel megegyező hardveren.
- **DMZ:** „Demilitarized Zone” („biztonsági övezet”). Független hálózati szegmens a hálózatok megbízhatatlannak tekintett külső, és védendő belső része „között”. A tűzfal a DMZ-ben elhelyezkedő hálózati eszközökhöz és erőforrásokhoz mind a belső, mind a megbízhatatlannak tekintett külső zónából engedélyezi a hozzáférést, de megakadályozza, hogy a külső zónából bármilyen kérés vagy hozzáférési kísérlet eljusson a belső hálózatra.
- **Image** (image fájl - „másolati kép adatállomány formájában”): Az eredeti partícióról, diszkról készült pontos másolat. Készítése során az eredeti partíció, diszk egyetlen összefüggő adatfolyamként jelenik meg, amely alapján – az első szektortól az utolsóig haladva – bitről bitre áll elő a másolati kép (az image fájl).
- **Inkrementális mentés:** Az utolsó mentés óta bekövetkezett változások rögzítése.
- **Központi mentés:** Mentés több rendszerről egy, központi szerveren futó szoftverrel. A központi szerverhez egy vagy több mentőegység, diszk-rendszer kapcsolódik.
- **Lokális (helyi) mentés:** Lokális mentés esetén a mentést végző szoftver a mentendő rendszeren fut, és csak annak az eszköznek a mentését szolgálja.

- **Megőrzési idő:** A megőrzési idő azt az időtartamot határozza meg, ameddig az adott mentési generációt meg kell őrizni. A megőrzési időt célszerű a mentési generációkkal és időegységben is megadni. Az előbbi oly módon, hogy hány egymást követő mentési generációval kell rendelkezni egy időben. Például, ha a napi mentés 7 generációját kell megőrizni, akkor a hétfői mentést a következő hét hétfőjén kell felülírni.
- **Mentés gyakorisága:** Azt határozza meg, hogy milyen időközönként kell mentést készíteni. Pl.: Óránként – 55 perckor, Naponta – 18 órakor, Hetente – pénteken 18 órakor, Havonta – 1-én 18 órakor, Évente – Január 1-én 18 órakor stb.
- **Mentési generáció:** A mentési generáció a kijelölt adatoknak, könyvtáraknak, állományoknak a mentési gyakoriságnak megfelelően, különböző időpontokban készített másolatai.
- **Mentési napló:** Minden mentést dokumentálni kell elektronikusan vagy papíron a mentések és mentési adathordozók követhetőségének érdekében. Ha a mentést végző szoftver nem végzi el a naplózást, akkor a naplót kézzel kell vezetni.
- **Mentő drive:** Mentést végző hardver eszköz.
- **Mentő szoftver:** Adatmentések, visszaállítások automatizálására szolgáló többkomponensű szoftverrendszer.
- **On-line médiatárolás:** A mentési médiák a mentőszerver számára médiakezelésre, visszaállításra hozzáférhetőek.
- **Off-line médiatárolás:** A mentési médiák tárolása olyan külső helyszínen, ahol a mentőszerver számára médiakezelésre, visszaállításra nem hozzáférhetőek.
- **Patch:** Programjavító csomag.
- **Példányszám:** Azt határozza meg, hogy egy mentési generációból hány darabbal kell rendelkezni.
- **Slot:** Tape Library-ben szalagok elkülönített tárolására szolgáló tároló hely.
- **Szalagos média:** Adatmentésre, lineáris adattárolásra szolgáló hardver eszköz.
- **Autoloader:** Több szalag tárolására, mentések során történő automatikus cseréjére szolgáló hardver eszköz.
- **Teljes („full”) mentés:** Olyan mentés, amelynek során minden adatról készül másolat.

## A szabályzathoz kapcsolódó szerepkörök

A mentési eljárásához az alábbi szerepkörök tartoznak:

- Mentési adminisztrátor
- Infrastruktúra rendszergazda
- Alkalmazás rendszergazda
- Üzemeltetési vezető
- Adatgazda
- Felhasználó

## A mentési és visszaállítási rendszerrel szemben támasztott követelmények

A mentéshez kapcsolódó követelményrendszer egyrészt meghatározza a mentésben résztvevő adatok körét, másrészt definiálja azokat az irányelveket, melyek figyelembevételével a mentési és visszaállítási eljárást, a mentett adatok kezelését, tárolását, megsemmisítését kell végezni.

## Mentendő adatok köre

A Bástya Millenium Zrt. mentendő adatait, alkalmazásait az alábbi felsorolás tartalmazza:

Kiszolgáló	Mentés módja	File mentés során mentendő adatok köre

## Mentési irányelvek

1. A mentés célja, hogy biztosítsa a mentésre kerülő informatikai eszközökön tárolt adatok sértetlenségét akkor is, ha az eredeti adattároló berendezéseken azok logikai, vagy fizikai probléma miatt megsérülnek.
2. A mentésnek nem célja az adatvesztés teljes kizárása, de célja biztosítani azt, hogy az utolsó sikeres mentésből a működőképes rendszer és minden a működéshez szükséges, tárolt adat visszaállítható legyen.
3. A kialakított mentési stratégiának biztosítania kell, hogy tetszőleges meghibásodás esetén a rendszer és az adatok az előző napi, illetve mentett állományok alkalmazásával visszaállítható legyen.
4. A mentési rendszernek biztosítania kell, hogy az adat visszatöltés és az informatikai szolgáltatás helyreállítási ideje, tetszőleges meghibásodás esetében se haladja meg az üzletmenet folytonossági tervben („BCP”) meghatározott kiesés időt.
5. A mentő rendszerre a Bástya Millenium Zrt.-nek rendelkeznie kell érvényes támogatási szerződéssel, amely biztosítja az új szoftververziók használatának jogát, valamint garanciális ügyintézkést és hibajegy feladás lehetőségét.

Az alábbi szabályokat figyelembe kell venni a mentési infrastruktúra kialakításakor, valamint a mentési rendszerek konfigurálásakor. A mentéseket minden esetben az alábbi általános követelmények betartásával kell elvégezni:

1. A heti egy alkalommal készülő full mentések médiáit ki kell venni és eltérő telephelyen kell tárolni.
2. A mentendő állományok meghatározásakor a következő irányelveket kell szem előtt tartani:
  - a. Minden olyan adatot menteni kell, amely szükséges az alkalmazások és/vagy üzleti folyamatok hibamentes működéséhez
  - b. Felhasználók magáncélú állományait nem szabad menteni.
  - c. A mentendő adatmennyiséget a fentiek figyelembevételével minimalizálni kell.
3. A mentések gyakoriságát és időzítését úgy kell meghatározni, hogy az adatvesztési intervallumok a lehető legkisebbek legyenek, de a mentések végrehajtása csak a lehető legkisebb mértékben zavarja meg a mentendő alkalmazás/rendszer és a környezeti infrastruktúra működését.
4. Amennyiben egyéb szabály nem rendelkezik a mentendő állományokról, úgy a mentéseket a következő forgási idővel kell végezni:
  - a. A naponta készülő mentéseket mentéseket 7 napig kell tárolni.
  - b. A hetente készülő full mentések független, biztosított, zárt helyszínen kerülnek tárolásra.
  - c. Az adatbázis tranzakciós naplókról készített mentéseket a következő adatbázismentésig kell tárolni.
5. A mentési ablakot a fenti elvek figyelembevétel mellett a lehető legszűkebbre kell venni.
6. Lehetőség szerint törekedni kell a mentések automatikus, időzített indítására.
7. A mentéseket minden esetben naplóztatni kell.
8. A mentések futási eredményét naponta ellenőrizni kell. A mentési rendszert fel kell készíteni arra, hogy a mentések lefutásáról, illetve az esetleges hibákról riasztást generáljon a felelősök számára.

## ***Az operációsrendszerek mentése***

1. Operációsrendszerek mentése esetében törekedni kell a teljes bitkép alapú mentésre.
2. Amennyiben ez nem valósítható meg, a mentést úgy kell elvégezni, hogy egy standard operációsrendszer telepítés és a mentett állományok visszatöltése képes legyen az eredeti környezetet visszaállítani.
3. Lehetőleg olyan megoldást kell választani, amely biztosítja az operációsrendszer éles futásidőben történő mentését.
4. Operációsrendszer mentését minden olyan esetben el kell végezni, amikor a rendszerben olyan módosítás történik, amely eltér az utolsó mentett állapottól és befolyásolja a funkcionális működés zavartalanságát egy esetleges visszaállítás esetén.
5. Operációsrendszer mentést kell végrehajtani minden hardverváltoztatás, illetve szoftver verzióváltás előtt.

## ***Az alkalmazás állományok mentése***

1. Az alkalmazás telepítőkészletének aktuális verzióját, és az alkalmazás dokumentációját minden esetben elérhető helyen kell tárolni.
2. Az alkalmazás állományait csak a következő esetekben kell menteni:
  - a. Az alkalmazás visszaállítása ezt szükségessé teszi.
  - b. Az alkalmazás visszaállítása gyorsabban megvalósítható visszatöltéssel, mint újratelepítéssel.
  - c. Az alkalmazás olyan adatokat tárol, amelyek csak mentésből állíthatók vissza.
3. Az alkalmazások állományait legalább heti rendszerességgel kell menteni, illetve minden esetben, amikor a rendszerben olyan módosítás történik, amely eltér az utolsó mentett állapottól és befolyásolja a funkcionális működés zavartalanságát egy esetleges visszaállítás esetén.
4. Az alkalmazás nem javítható sérülésekor az alkalmazást újra kell telepíteni.

## ***Az adatbázisok mentése***

1. Az adatbázisokat a hét minden napján legalább egyszer menteni kell.
2. Minden esetben törekedni kell arra, hogy az adatbázis konzisztens állapotban kerüljön mentésre.
3. Amennyiben a mentendő állományok mérete, a rendelkezésre álló mentési idő és a mentési tárterület erre lehetőséget biztosít, mindig teljes körű mentést kell alkalmazni.
4. A működő adatbázisokat vagy az adatbázisba épülő mentő szoftver alkalmazásával, vagy fájlmentéssel kell menteni. (A fájlt az adatbázis saját eszközeivel kell exportálni - mentésre előkészíteni.)

## ***Fájlmentés***

1. A fájlokat lehetőleg naponta kell menteni. Ettől eltérni, csak olyan állományok esetében lehet, amelyek nem módosulnak naponta, illetve akkor, ha a mentendő területen új állományok sem keletkeznek.
2. Hacsak nem szól ellene nyomós érv, a fájlmentéseket inkrementálisan kell végrehajtani a mentéshez szükséges hely, és idő minimalizálása érdekében.

## ***A mentett adatok és mentési médiák kezelése***

### **A mentett adatok logikai védelme**

1. A mentést végző szoftverhez való hozzáférést jelszóval kell védeni, biztosítva ezzel azt, hogy csak az arra jogosult férhessen hozzá. A mentési rendszerhez csak a Mentési adminisztrátor és az Üzemeltetési vezető férhet hozzá.

2. A mentett éles adatok logikai hozzáférés védelmének szintje meg kell, hogy egyezzen az eredeti éles adatok hozzáférés védelmének szintjével.

## A mentett adatok fizikai védelme

1. A mentett éles adatok fizikai hozzáférés védelmének szintje meg kell, hogy egyezzen az éles adatok hozzáférés védelmével.
2. A mentési adathordozó eszközök tárolása csak megbízhatóan zárt helyiségben történhet, amelynek kialakítása során biztosítani kell a következőket:
  - a. az adathordozó gyártója által előírt környezeti feltételeket (hőmérséklet, relatív páratartalom, pormentesség),
  - b. természeti csapások elleni védelmet.
  - c. A helyiséget el kell látni füst- és tűzjelző készülékkel.
  - d. Távollét esetén a helyiséget zárva kell tartani.
  - e. A heti full mentések legalább egy példányát a mentésre került rendszertől eltérő helyszínen, de az eredetivel megegyező biztonsági körülmények között kell tárolni.

## A mentési médiák kezelése

1. A médiák használati ideje nem lehet hosszabb, mint a gyártó által szavatolt használhatósági idő 90%-a.
2. Biztonsági másolat készítésére idegen (nem Bástya Millenium Zrt. tulajdonú) mentési média nem használható.
3. A mentési médiákat selejtezésük után nem lehet újrafelhasználni. A médiákat meg kell semmisíteni. A megsemmisítésről jegyzőkönyvet kell készíteni.
4. A médiákat használatbavételkor egyértelműen azonosítani kell.
5. Az off-line tárolt médiák egyértelmű azonosítását egységesen kialakított médiacímkézéssel kell megoldani.

## A mentési infrastruktúra leírása

A Bástya Millenium Zrt. mentési infrastruktúrája az alábbi elemekből épül fel:

### Mentő kiszolgáló

Hostnév:

IP cím:

Operációsrendszer:

Mentő szoftver:

### Autoloader

Típus:

Média típusa:

IP cím:

## A mentési logika leírása

A mentések ütemezését az alábbi táblázat tartalmazza:

Mentési job	Mentendő kiszolgáló	Mentés típusa	Mentés indítása

A Bástya Millenium Zrt. igen / nem rendelkezik másodlagos telephellyel (disaster site), így a teljes infrastruktúra megsemmisülése esetén ezekből a független mentésekből kell helyreállítani a szolgáltatásokat.

## Adatvesztési ablakok:

A mentési rend által szavatolt adatvesztési ablakok (RPO) az alábbiak:

Egy alkalmazás, vagy kiszolgáló meghibásodása esetén a maximális adatvesztési ablak 24 óra.

A teljes infrastruktúra megsemmisülése esetén a maximális adatvesztési ablak 1 hét.

## A visszaállítás szabályozása

1. Adat visszatöltését pl. sérülés, törlés, hibás módosítás miatt a felhasználó, az adatgazda, vagy az Üzemeltetési Vezető kérheti a Mentési Adminisztrátortól.
2. A visszaállítási kérelem a sürgösségre való tekintettel, történhet telefonon, de minden esetben írásban is meg kell erősíteni.
3. A visszaállítás során pontosan meg kell határozni azokat az állományokat, adatbázisokat, amiket vissza kell állítani.
4. A visszaállítási eljárásra az alábbi szabályok vonatkoznak:
  - a. Az eljárás nem veszélyeztetheti a visszaállítás utáni működést.
  - b. A visszaállításra kerülő adatmennyiség méretét, és/vagy számosságát minimalizálni kell
  - c. Minél kevesebb állomány kerüljön lecserélésre.
5. Amennyiben más időpont nincs meghatározva, - az utolsó mentést kell választani.
6. A visszaállítást általában az eredeti diszk területre kell elvégezni. Az eredeti helyszínt ellenőrizni kell, hogy ne maradjon olyan fontos állomány, amelyet a visszaállítás korábbi állapotúra cserélne.
7. Amennyiben nincs lehetőség az eredeti helyszín kijelölésére, úgy olyan ideiglenes helyszínt kell választani a visszaállítás céljával, amelyen biztosítva van a visszaállított adatok hozzáférés védelme és a rendelkezésre álló terület elégséges a visszatöltendő adatmennyiség számára.
8. Adatbázis visszaállítása vagy csak az eredeti helyszínen, a tartalék környezetben illetve teszt környezetben vagy egy ideiglenesen telepített, az eredetivel megegyező verziójú adatbázis kezelőn történhet.
9. Éles környezetben történő visszaállításkor, a visszaállítást nem időzítve, hanem kézi indítással kell elvégezni.

## Egyes állományok visszaállítása

Egyes állományok két módon állíthatók helyre:

Tipikus esetben az állományszintű mentésből, a kért állomány, vagy könyvtár az eredeti, illetve egyéb meghatározott helyszínrre visszatölthető.

Amennyiben a visszaállítandó állományról nem készül állományszintű mentés, úgy az adott szerver image mentéséből egy offline teljes állapot állítható vissza. Ebből az ideiglenes állapotból a kért állomány kimásolható. Az offline helyreállítások során kiemelkedően fontos, hogy a visszaállított rendszer ne csatlakozhasson a Bástya Millenium Zrt. belső hálózatához, mivel az eredeti kiszolgáló ott éles környezetben működik.



## Teljes rendszer visszaállítása

Amennyiben az eredeti kiszolgáló nem működőképes, az utolsó mentett teljes állapot kerül visszaállításra a teljes, image alapú mentésből. A visszaállítás után a korábbi kiszolgáló állományait törölni kell a storage tárterületről. Teljes visszaállítás tipikusa az alábbi esetekben történik:

- Disaster esemény melynek során a kiszolgáló működése helyreállíthatatlanul megsérült.
- Rendszerfrissítések után, mikor az adott új verzió nem megfelelően működik és a hiba a helyreállítási időablakban nem orvosolható.

## A mentő szerver mentése és visszaállítása

A mentő szerver mentése kiemelt jelentőségű, mivel a mentő szoftverben tárolt catalogue állomány fontos a mentések gyors visszaállítása érdekében. A szerverből ezt az állományt kell rendszeren menteni.

A mentett állomány visszamásolásával a szerver disaster esetén egy új operációs rendszer és mentőszoftver telepítés után a mentési állapotra helyreállítható.

## A szerepkörök feladatai a mentés-visszaállítás során

### Mentési adminisztrátor

A mentési adminisztrátor felelős:

- Az általa felügyelt mentő rendszerek hibamentes működéséért.
- A mentések megfelelő időzítéssel történő lefutásáért.
- A mentett adatok biztonságos körülmények között történő tárolásáért és kezeléséért, valamint
- a mentésekből történő visszaállíthatóság biztosításáért.

A mentési adminisztrátor nem tehető felelőssé a mentett adatok teljességéért és a visszaállítás sikertelenségéért abban az esetben, ha az alkalmazás rendszergazdától, vagy fejlesztőktől a mentéshez megküldött adatok köre hiányos vagy pontatlan és ezért a visszaállítás nem hajtható végre.

A mentési adminisztrátornak rendelkeznie kell a felügyelete alá tartozó informatikai eszközök kezeléséhez szükséges szakmai ismeretekkel.

Tudását a technológia és az eszközök változásával párhuzamosan meg kell újítani.

### Alkalmazás rendszergazda

Az alkalmazás rendszergazda feladatai:

Az általa üzemeltetett, illetve fejlesztett alkalmazás mentéséhez szükséges állományok és elérési utak listáját meg kell küldenie a Mentési Adminisztrátornak, illetve ezek módosulása esetén a mentési információkat aktualizálnia kell.

Visszaállítás során ellenőriznie kell, hogy a visszaállított rendszer, vagy komponens működőképes e.

A mentési job-ok ütemezéséről egyeztet a Mentési Adminisztrátorral, az alkalmazás működési, terheltségi időszakainak figyelembevételével.

## Üzemeltetési vezető

1. Az Üzemeltetési Vezető felelős azért, hogy a mentési rendszer hibamentes, megbízható működéséhez és működtetéséhez szükséges erőforrások, információk, valamint hardver és szoftver feltételek rendelkezésre álljanak.
2. Biztosítania kell a mentő eszközök karbantartását.
3. A mentő eszközök meghibásodása esetén, döntést hoz a mentések átütemezéséről, a mentési adminisztrátortól kapott információk alapján.
4. Biztosítania kell, hogy a mentő rendszerek jogtiszta szoftverekkel rendelkezzenek és, hogy a rendszerek működtetését érvényes szerződés alapján, mind a gyártó, mind egy felkészült szolgáltató támogassa.

## Felhasználó

1. A felhasználó felelős az adatvesztés valószínűségének csökkentéséért azzal, hogy a saját hatáskörében kezelt fontos adatok (pl. hivatalos dokumentum) legalább egy példányát a fájlserveren tárolja, amelyről a jelen szabályzat szerint automatizált biztonsági másolat készül.
2. A felhasználó magán (nem Bástya Millenium Zrt.) adatot a hálózati adathordozókon nem tárolhat, s tudatosan kerülnie kell felesleges másolatok tárolását olyan Bástya Millenium Zrt. adatról, amely egyébként központi, hálózati adathordozóról elérhető.
3. Visszaállítás kérése esetén a visszaállítás után Felhasználó feladata az általa igényelt állományok meglétének, illetve az általa használt alkalmazás működőképességének felhasználói szintű ellenőrzése.

## Az utasítás felülvizsgálata és a szabályoktól való átmeneti eltérés dokumentálása

Ha a szabályzat betartása objektív akadályba ütközik, akkor rendelkezéseitől az Üzemeltetési vezető írásos engedélyével el lehet térni. Az utasítástól való minden eltérést jegyzőkönyvben dokumentálni kell

### 1. Melléklet: Szerepkörök és személyek összerendelése

Szerepkör	Személy	Elérhetőség
Mentési adminisztrátor		
Infrastruktúra rendszergazda		
Alkalmazás rendszergaza		
Üzemeltetési vezető		
Ügyvezető		