
INFORMÁCIÓBIZTONSÁGI KÉZIKÖNYV KIVONAT A MINDENKORI HATÁLYOS IBK-BÓL

Külső használatra

***Szabályzat kidolgozásáért és karbantartásáért
felelős:***

*Információbiztonsági Felelős
Informatika igazgató
Integrált Irányítás tanácsadó
HR és Belső Szolgáltatások igazgató*

Szabályzat kiadásáért felelős:

Jog és Szabályozás vezető

Jóváhagyta:

*Vezérigazgató
Elnök-vezérigazgató*

Tartalomjegyzék

1.	Az információbiztonság rendszere	3
2.	FGSZ Zrt. Információbiztonsági elvárások	3
2.1.	FGSZ Zrt. adatok védelme	3
2.2.	Információbiztonság tudatosítása, oktatása és képzése	3
2.3.	Feladatkörök szétválasztása.....	4
2.4.	Fegyelmi eljárás	4
2.5.	A tárolt információvagyon védelme, a vagyonelemek kezelése.....	4
2.6.	A rendszerek hozzáférési jogosultságainak kezelése, hozzáférés-felügyelet	4
2.7.	Felhasználó hitelesítés külső csatlakozások esetén, a hálózati szolgáltatások biztonsága	4
2.8.	Bizalmassági vagy titoktartási megállapodások.....	5
2.9.	Az információbiztonsági incidensek kezelése	6
2.10.	Az információbiztonsági incidensek és javítások kezelése	6
3.	FGSZ Zrt. Információbiztonsági ajánlások	6
3.1.	A rendszerek hozzáférési jogosultságainak kezelése, hozzáférés-felügyelet	6
3.2.	A hozzáférés-felügyelettel kapcsolatos üzleti követelmények	8
3.3.	Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz.....	8
3.4.	Védelem a rosszindulatú kódok ellen	8
3.5.	Naplózás és megfigyelés	8
4.	Mellékletek.....	8

1. AZ INFORMÁCIÓBIZTONSÁG RENDSZERE

Az FGSZ Zrt., mint a magyarországi nagynyomású földgázszállító rendszer üzemeltetője, alapvető feladata az országos gázellátáshoz szükséges gázmennyiség folyamatos biztosítása, az ügyfelek kiszolgálása. Az FGSZ Zrt. Informatika által működtetett rendszerek és alkalmazások, az általa kezelt adat- és információvagyon fenntartásának célja a működési engedélyhez kapcsolódó feladatok ellátása. A feladatellátásnak vannak olyan elemei, amelyeknek az adott év bármely napjának bármely időpontjában működőképesnek kell lennie. Az Informatika működésével és működésfolytonosságával kapcsolatosan az alapvető elvárásokat ez a 365 nap / 24 óra típusú készenlét és rendelkezésre állás határozza meg. Az FGSZ Zrt. működését - többek között - a 2008. évi XL. törvény a földgázellátásról (a továbbiakban GET) szabályozza, melynek 10.§ előírja az ISO/IEC 27001 szabványnak való megfelelést. Ezért FGSZ Zrt. partnereinek is a ISO/IEC 27001 információbiztonsági irányítási rendszer szabvány betartását javasolja. Az Információbiztonsági Kézikönyv (röviden: IBK) a Társaság minden munkavállalójára és **szerződéses partnerére vonatkozó, kötelező érvényű utasítás.**

Másrészt az FGSZ Zrt. **ajánlásokat** fogalmaz meg partnerei felé, melyeket a partnereinek a saját működésük során célszerű betartaniuk.

1.1. Az információbiztonság három alapvető összetevője

- Bizalmasság: az információt csak az legyen képes elolvasni, aki arra jogosult.
- Sértetlenség: az információt csak az módosíthassa vagy törölhesse, aki arra jogosult, továbbá az adat hiteles forrása bizonyítható legyen.
- Rendelkezésre állás: az arra jogosult felhasználó a szükséges információhoz a megfelelő helyen és időben hozzáférhessen.

2. FGSZ ZRT. INFORMÁCIÓBIZTONSÁGI ELVÁRÁSOK

Az FGSZ Zrt **elvárásokat** fogalmaz meg a partnerei számára, melyeket az FGSZ Zrt. rendszerek fejlesztése, üzemeltetés támogatása, hardver és szoftver licence szállítása, valamint szolgáltatás nyújtása során be kell tartaniuk.

2.1. FGSZ Zrt. adatok védelme

FGSZ Zrt. partnereinek minden lehetséges intézkedést el meg kell tenni annak érdekében, hogy FGSZ Zrt. adatai csak az arra jogosultak részére legyen elérhető

2.2. Információbiztonság tudatosítása, oktatása és képzése

FGSZ Zrt. partner felé elvárás, hogy rendszeresen tartson felhasználói képzéseket munkavállalói/alvállalkozói részére. A felhasználói képzések célja, hogy a felhasználók tájékozottak legyenek az Információbiztonsági követelményekkel kapcsolatban, és tudatában legyenek a követelmények figyelmen kívül hagyásának következményeivel és veszélyeivel. Az oktatásnak ki kell térnie az Információbiztonsági, adatvédelmi folyamatokra, szabályozásokra és az adatfeldolgozás célszerű módszereire ezzel csökkentve a biztonsági kockázatokat.

2.3. Feladatkörök szétválasztása

FGSZ Zrt. partner válassza szét az informatikai és telekommunikációs üzemeltetés- és a fejlesztés feladatköröket.

Az FGSZ Zrt. partner Informatika munkatársak feladatainál el kell különíteni egymástól a fejlesztők, alkalmazásüzemeltetők és rendszeradminisztrátorok felelősségét, feladatkörét.

2.4. Fegyelmi eljárás

FGSZ Zrt. partner külső partner felé ajánlás, hogy azokkal a munkavállalóival/alvállalkozóival szemben, akik szándékosan és tudatosan megsértik az Információbiztonsági szabályokat, tevékenységükkel szándékosan kárt okoznak, fegyelmi eljárás kezdeményezhető.

2.5. A tárolt információvagyon védelme, a vagyonelemek kezelése

Az informatikai rendszerben kezelt adatok védelmét az adatok keletkezésének, feldolgozásának, forgalmazásának, tárolásának és selejtezésének teljes folyamata során biztosítani kell. Mivel az információvagyron szerves része az az eszközpark, amelyen az adatok és információk keletkeznek, vagy módosulnak, az FGSZ Zrt. területére érkező, illetve azt elhagyó informatikai eszközök mozgását, valamint az épületeken belüli, illetve a telephelyek közötti eszközmozgásokat dokumentálni kell. A dokumentációs tevékenységnek ki kell terjednie:

- A beérkező eszközök, alkatrészek nyilvántartásba vételére,
- A külső munkára kiadott eszköz vagy alkatrész használatba adására,

2.6. A rendszerek hozzáférési jogosultságainak kezelése, hozzáférés-felügyelet

Biztosítani kell, hogy az FGSZ informatikai infrastruktúráját kizárólag az erre jogosult felhasználók és az erre kijelölt információs erőforrások használhatják.

Követelmények:

- Külső szerződött partnerek dolgozói, megbízottjai az FGSZ informatikai rendszeréhez való jogosultságot kizárólag az Informatika vezető jóváhagyása esetén kaphatnak. A külsős, FGSZ Zrt. szerződött partner kitöltve és aláírva juttatja el a titoktartási nyilatkozatot az FGSZ-es kapcsolattartója segítségével az FGSZ Zrt. Belső rendszerében található „Ilgények kezelése” szabályzat szerint.

2.7. Felhasználó hitelesítés külső csatlakozások esetén, a hálózati szolgálatások biztonsága

Külső bejelentkezés (FGSZ Zrt. belső hálózat távoli elérése) esetén a felhasználónak tudnia kell, hogy a külső bejelentkezési helyről használható kiterjesztett elérési jogok gondatlan használat esetén sokkal veszélyesebb biztonsági rést nyitnak meg, mint a belső hálózatról bejelentkezők.

A FGSZ Zrt. belső hálózat távoli elérését az FGSZ Zrt. Informatika vezetője engedélyezi.

A rendszerbe való belépés csak a belépő személy technikai azonosítása és hitelesítése (pl. ugrókédos token) után lehetséges.

A FGSZ Zrt. távoli bejelentkezést a rendszer ellenőrzi és naplózza. A naplózás dokumentumait az FGSZ Zrt. Információbiztonsági Felelős ellenőrzi. A távoli eléréseket a nem FGSZ. Zrt. alkalmazottak részére, lehetőség szerint, „távoli asztal” kapcsolattal kell biztosítani.

VPN használat követelményei:

- A külső szerződött partnerek kizárólag érvényes szerződés alapján kapnak hozzáférést az FGSZ Zrt. informatikai infrastruktúrájához.
- A csatlakozó számítógépeknek meg kell felelniük a védelmi szoftverekkel kapcsolatos követelményeknek (pl. rosszindulatú programok észlelése/tiltása, tűzfal, rendszeres információbiztonsági szoftverfrissítések).
- A külső felek, FGSZ Zrt. rendszer hozzáférési jogosultságai kizárólag határozott időtartamra vonatkozhatnak, a jogosultság lejáratá az FGSZ Zrt. központi címtárban kerül rögzítésre.
- Az FGSZ Zrt.-nek jogában áll megvonni a korábban megadott hozzáférési jogot amennyiben az érintett fél biztonsági incidenst idéz elő.

2.8. Bizalmassági vagy titoktartási megállapodások

Minden FGSZ Zrt. szerződött külső partner köteles a munkája során tudomására jutott üzleti titoknak minősíthető adatot vagy információt megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot vagy információt, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a munkáltatóra vagy más személyre hátrányos következménnyel járhat.

Az alkalmazási rendszerek bevezetésében és felhasználásában közreműködő külső FGSZ Zrt. partner titoktartásra kötelezett.

A titoktartási kötelezettség kiterjed:

- a FGSZ Zrt. Társasági információkra
- a bevezetésben közreműködő vállalatról szerzett információkra és
- az FGSZ Zrt. alkalmazási rendszerekkel kapcsolatos információkra.

Az FGSZ Zrt. partnerrel szerződéses vagy egyéb kapcsolatba kerülő külső személyekre a titoktartási kötelezettség és felelősség vállalás ugyanúgy vonatkozik. Ezen rendelkezés betartásának biztosítása érdekében az FGSZ Zrt. partner részéről szerződést kötő egység kötelezettsége annak biztosítása, hogy a szerződések tartalmi elemét képezze a szerződő partner titok- és adatvédelmi nyilatkozata, kötelezettségvállalása.

Az FGSZ Zrt. informatikai hálózatán, illetve informatikai eszközein munkát végző külső partner dolgozói is titok- és adatvédelemre, illetve titoktartási nyilatkozat tételére kötelezettek.

Az alkalmazási rendszerek bevezetése és működtetése kapcsán az FGSZ Zrt.-vel kapcsolatba kerülő külső szervezetek, személyek a FGSZ Zrt. kötött szerződésben felelősséget kell, hogy vállaljanak azért, hogy a tudomásukra jutott és az FGSZ Zrt.-t érintő üzleti titkokat semmilyen módon fel nem használják, harmadik személy részére át nem adják, azokról másolatot nem készítenek és biztosítják, hogy mindezen adatokba való betekintés kizárólag a szerződésben foglalt célokat szolgálják.

Minden munkavállalónak és az FGSZ Zrt.-vel kapcsolatba kerülő olyan külső személynek, aki a FGSZ Zrt. partnerre vagy munkavállalóira vonatkozóan bármilyen adatot kezel, titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája során tudomására jutott, az FGSZ számára értéket jelentő információt sem a munkavégzése ideje alatt, sem azt követően nem hozza harmadik fél tudomására.

Új FGSZ Zrt. partner felhasználók esetében a nyilatkozatot az azonosító kiadása előtt kell aláírni.

2.9. Az információbiztonsági incidensek kezelése

Az FGSZ Zrt. partnernek biztosítani kell az Információbiztonsági incidensek kezelését.

Követelmények:

- Minden potenciális – az FGSZ Zrt-vel összefüggő - Információbiztonsági incidenst és gyengeséget haladéktalanul jelenteni kell az FGSZ Zrt. Informatika vezetőjének és az Információbiztonsági Felelősnek, ezen az email címen: **IBF@fgsz.hu**

A biztonsági incidensek kezeléséért az FGSZ Zrt. Információbiztonsági Felelős és az FGSZ Zrt. Informatika vezetője felel.

2.10. Az információbiztonsági incidensek és javítások kezelése

Biztonsági incidensnek minősülnek azok az üzemeltetési események, amelyek lehetőséget adtak nem legitim adat módosulására, személyes- vagy üzleti adatok kompromittálódására, csökkentik a rendelkezésre állás szintjét vagy sérül a bizalmasság vagy a sértetlenség. Rendkívüli esemény vagy incidens esetén, annak tényéről az Információbiztonsági Felelős haladéktalanul tájékoztatja a FGSZ Zrt. Informatika vezetőjét és a FGSZ Zrt. Társasági Biztonság Vezetőt.

Az FGSZ Zrt. minden szerződött partnerének kötelessége a rábízott, illetve a környezetében megjelenő adatok és információk biztonságos kezelése, a rosszindulatú módosítások, az adat- és/vagy információvagyron kiszivárgásnak megakadályozása. Ennek érdekében minden szerződött partner kötelessége az olyan cselekmények megakadályozása, amelyek „fokozott”, vagy magasabb védelmi osztályba sorolt adatok, vagy információk kiszivárgásához vezethet.

Minden szerződött partner kötelessége, hogy:

- a felismert vagy felismerni vélt biztonsági esemény,
- a felismert vagy felismerni vélt védelmi gyengeség, biztonsági rés, sérülékenység,
- a tapasztalt Információbiztonsági szempontból nem megfelelő magatartás,
- vagy bármilyen bizalmas információ kiszivárgásnak

jelentése az FGSZ Zrt. Informatika vezetőjének és az Információbiztonsági Felelősnek, az **IBF@fgsz.hu** email címen.

3. FGSZ ZRT. INFORMÁCIÓBIZTONSÁGI AJÁNLÁSOK

Az FGSZ Zrt. **ajánlásokat** fogalmaz meg partnerei felé, melyeket a partnereinek a saját működésük során célszerű betartaniuk, annak érdekében, hogy FGSZ Zrt. információs rendszerei, adatai semmilyen módon ne kompromittálódjanak. Ezek az ajánlások az alábbiak.

3.1. A rendszerek hozzáférési jogosultságainak kezelése, hozzáférés-felügyelet

- A felhasználó hitelesítésnek egyértelműnek kell lennie (nem javasolt a „nem személyhez rendelt” vagy „közös felhasználó azonosító” használata – a tényleges információkat nem tartalmazó, elkülönített oktatási vagy teszt környezet kivételével - egy-egy felhasználó azonosító csak egyetlen felhasználóhoz rendelhető).

- Az alkalmazott hitelesítési módszerrel szemben támasztott FGSZ Zrt követelmények:
 - **RFID rendszerre** vonatkozó jelszó előírások, vagyis, ha az FGSZ tartományi jelszót RFID szerver bejelentkezésre is használjuk, akkor használható karakterek:
 - kis- és nagybetűk,
 - számok,
 - **a speciális karakterek közül a következők:** + - () = % ! [] () / . , ; : _ * | # { } ?
 - **Normál és rendszergazda** (admin) felhasználó azonosító esetén:
 - a jelszó minimális hosszúsága privilegizált jogok nélküli, **normál felhasználó** esetén minimum 12 karakter,
 - **rendszergazda** (privilegizált) felhasználó esetén minimum 16 karakter, és amennyiben van rá lehetőség multifaktor autentikációt kell használni,
 - jelszó élettartama maximum 180 nap,
 - jelszó összetettsége (legalább egy kis- és nagybetűt ÉS/VAGY egy számot ÉS/VAGY egy speciális karaktert kell tartalmaznia),
 - jelszó történeti adatai (a legutóbbi 24 jelszó nem használható fel újra),
 - az alapértelmezett vagy kezdeti jelszó kezelése: az alapértelmezett vagy kezdeti jelszót az első bejelentkezés során módosítani kell,
 - a sikertelen hitelesítés kezelése (maximum 8 sikertelen bejelentkezési kísérlet után az adott felhasználó azonosító legalább 15 percre letiltásra kerülhet),
 - A jelszó minimális élettartama 24 óra (jelszótárolás után ennyi időnek el kell telnie a következő jelszótárolásig).
 - **Service/Technical Account/** (szerviz/technikai felhasználó) vonatkozásában:
 - Jelen előírásokat az IBK v11 kihirdetésétől számított két éven belül kell bevezetni.
 - A jelszó minimális hosszúsága 32 karakter.
 - A jelszó élettartama maximum 2 év. A jelszó lejáratot technikai intézkedésként nem kell beállítani az adott rendszerben, azonban adminisztratív intézkedésként jelen IBK előírásai alapján be kell tartani.
 - A jelszó összetettsége, komplexitása (legalább egy kis- és nagybetűt ÉS/VAGY egy számot ÉS/VAGY egy speciális karaktert kell tartalmaznia).
 - Jelszó történeti adatai (a legutóbbi 24 jelszó nem használható fel újra).
 - A jelszó minimális élettartama 24 óra (jelszótárolás után ennyi időnek el kell telnie a következő jelszótárolásig).
 - Amennyiben a Gyártó nem javasolja vagy tiltja jelszócserét, akkor az adott rendszer mentesül a jelszótárolási kötelelem alól.

3.2. A hozzáférés-felügyelettel kapcsolatos üzleti követelmények

A nem adminisztrátor jogú felhasználók nem rendelkezhetnek olyan hozzáférési lehetőségekkel, amivel más felhasználók adminisztrálását lehet végezni.

3.3. Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz

A hálózati szolgáltatások használatára vonatkozó szabályokat munkakör/szerep, illetve esetenként egyedi jogok alapján célszerű a partnereinket meghatározni.

A hozzáférés megadása mindig igény alapján történjen, és a felhasználót bejelentkezéskor mindig azonosítani és hitelesíteni szükséges a hálózati hozzáférés biztosítása előtt.

3.4. Védelem a rosszindulatú kódok ellen

Javasoljuk az FGSZ Zrt. partnereinek, hogy informatikai rendszereikben csak az ellenőrizhető forrásból származó programokat használjanak.

A kritikus működési folyamatokat támogató rendszerek szoftverére és adattartalmára vonatkozóan csak ellenőrzött, tesztelt, hiteles változatot telepítsenek.

Az FGSZ Zrt. partnerek rendelkezzenek Katasztrófa Elhárítási Tervvel, mely tartalmazzon eljárást a rosszindulatú kód támadásaiból való helyreállításra, beleértve minden szükséges adat és szoftver mentését, továbbá a helyreállítási intézkedéseket.

3.5. Naplózás és megfigyelés

FGSZ Zrt. partnerek informatikai rendszereiben végrehajtott tevékenységek minden esetben kerüljenek naplózásra. A naplók mentése legyen része a mentési rendnek, a naplóállományok együtt őrződjenek meg az egyéb hasznos állományokkal. Biztosítani kell a naplóállományok védelmét illetéktelen módosítás, törlés ellen.

4. MELLÉKLETEK

Melléklet száma	Melléklet címe
1. sz. melléklet	A megfelelő hitelesítésre és jogosultságra vonatkozó szabályok