
INFORMÁCIÓBIZTONSÁGI KÉZIKÖNYV KIVONAT(IBKK) 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 igazgató

Jóváhagyta:

*Vezérigazgató
Elnök-vezérigazgató*

Tartalomjegyzék

1.	Az információbiztonság rendszere	3
1.1.	1.1. Az információbiztonság három alapvető összetevője, ezeket be kell tartani:	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	5
2.8.	Bizalmassági vagy titoktartási megállapodások.....	6
2.9.	Az információbiztonsági incidensek kezelése	6
2.10.	Az információbiztonsági incidensek és javítások kezelése	6
2.11.	Biztonságos szoftverfejlesztés	7
2.12.	A hozzáférés-felügyelettel kapcsolatos üzleti követelmények	8
2.13.	Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz.....	8
2.14.	Védelem a rosszindulatú kódok ellen	8
2.15.	Naplózás és megfigyelés	8
3.	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 és a Főmérnökség által működtetett rendszerek és alkalmazások, az általuk 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 és Főmérnökség 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 az ISO/IEC 27001 információbiztonsági irányítási rendszer szabvány betartását kéri, illetve a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény betartása jogszabályi kötelezettség. Az Információbiztonsági Kézikönyv (röviden: IBK) a szervezet minden munkavállalójára, az IBKK pedig **a szerződéses partnerére vonatkozó, kötelező érvényű utasítás.**

Az FGSZ Zrt. **kötelmeket** fogalmaz meg partnerei felé, melyeket a partnereinek a saját működésük során be kell tartaniuk.

1.1. 1.1. Az információbiztonság három alapvető összetevője, ezeket be kell tartani:

- 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 szükséges intézkedést meg kell tenni annak érdekében, hogy FGSZ Zrt. adatai és információi 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. külső partner felé elvárás, 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 és kiber-fizikai 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, hozzáférési felügyelet

Az FGSZ Zrt. részére nyújtott szolgáltatások során alkalmazott rendszereket biztonságos konfiguráció szerint kell kialakítani. Az alapértelmezett felhasználói fiókokat és jelszavakat módosítani kell, a nem szükséges szolgáltatásokat le kell tiltani, valamint a legkisebb jogosultság elvét kell alkalmazni.

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

Követelmények:

- Külső szerződött partnerek dolgozói, megbízottjai az FGSZ informatikai és kiber-fizikai rendszereihez való jogosultságot kizárólag az Informatika vezető és Főmérnök jóváhagyása esetén kaphatnak. A külsős, FGSZ Zrt. szerződött partner kitöltve és aláírva juttatja el a titoktartási nyilatkozatot az FGSZ-es kapcsolattartójához.
- A hozzáféréseknek egyértelműen személyhez rendelt, egyedi felhasználói azonosítón kell alapulniuk. Közös vagy nem személyhez rendelt felhasználói azonosító használata nem megengedett, kivéve az elkülönített, tényleges információkat nem tartalmazó oktatási vagy tesztkörnyezeteket. Egy felhasználói azonosító kizárólag egyetlen felhasználóhoz rendelhető.

Ajánlott hitelesítési és jelszókezelési beállítások

Az FGSZ Zrt. az alábbi hitelesítési és jelszókezelési gyakorlatok alkalmazását ajánlja partnerei számára:

- Felhasználónév és jelszó alapú hitelesítés esetén javasolt legalább 12 karakter hosszúságú jelszavak alkalmazása.

- Emelt jogosultságú (privilegizált) felhasználói fiókok esetében javasolt legalább 16 karakter hosszúságú jelszavak vagy azzal egyenértékű erősségű hitelesítési megoldások használata.
- Távoli hozzáférés, valamint privilegizált jogosultságok esetén javasolt a többfaktoros hitelesítés (MFA) alkalmazása.
- Javasolt a könnyen kitalálható, szótári alapú vagy ismert kompromittálódott jelszavak használatának tiltása.
- Javasolt a korábban használt jelszavak ismételt felhasználásának korlátozása.
- Az alapértelmezett vagy gyári jelszavakat javasolt az első használatot megelőzően vagy az első bejelentkezéskor megváltoztatni.
- Javasolt a sikertelen hitelesítési kísérletek számának figyelése és szükség esetén ideiglenes fiókzárolás vagy egyéb védelmi mechanizmus alkalmazása.
- Javasolt, hogy a jelszavak cseréje kompromittálódás gyanúja, biztonsági incidens vagy egyéb indokolt eset alapján történjen.

2.7. Felhasználó hitelesítés külső csatlakozások esetén, a hálózati szolgáltatások 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.

Az FGSZ Zrt. informatikai infrastruktúrájához történő külső vagy távoli hozzáférés kizárólag az FGSZ Zrt. által engedélyezett, biztonságos és titkosított kapcsolaton keresztül, valamint többfaktoros hitelesítés alkalmazásával történhet.

A FGSZ Zrt. távoli bejelentkezést a rendszer ellenőrzi és naplózza. A naplózás dokumentumait az FGSZ Zrt. Információbiztonsági Felelős ellenőrzi. Az FGSZ Zrt.-nél nem alkalmazott személyek részére a távoli hozzáférést lehetőség szerint távoli asztali kapcsolaton keresztül 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.
- A külső hozzáférés során kizárólag a feladat ellátásához szükséges jogosultságok biztosíthatók.
- A külső kapcsolatok kialakítása során kizárólag az iparági gyakorlat és az aktuális biztonsági ajánlások alapján biztonságosnak tekintett protokollok és kriptográfiai megoldások alkalmazhatók.

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 munkavállalóra 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.

2.11. Biztonságos szoftverfejlesztés

Amennyiben az FGSZ Zrt. részére alkalmazás-, rendszer-, interfész-, automatizálási vagy egyéb szoftverfejlesztési tevékenységet végez, azt biztonságos fejlesztési eljárások alkalmazásával hajtja végre.

A szerződéses partner által teljesítendő követelmények:

- a fejlesztés során az információbiztonsági követelményeket már a tervezési szakaszban figyelembe kell venni;
- biztonságos fejlesztési életciklus (Secure SDLC) alkalmazása;
- a fejlesztői, teszt- és éles környezetek elkülönítése;
- verziókezelő rendszer használata;
- a fejlesztés lezárását megelőzően biztonsági tesztelés végrehajtása, valamint az azonosított sérülékenységek kockázatarányos javítása;
- a fejlesztés során keletkező forráskód, konfigurációs állományok és egyéb fejlesztési információk megfelelő védelme.

Az FGSZ Zrt. által kezdeményezett, a szerződéses partner közreműködésével végrehajtott tevékenységek:

- a forráskód biztonsági célú átvizsgálása (SAST és/vagy manuális ellenőrzés) az FGSZ Zrt. információbiztonsági folyamatainak megfelelően;
- független biztonsági kódvizsgálat vagy egyéb biztonsági felülvizsgálat végrehajtása az FGSZ Zrt. kezdeményezésére;
- a szerződéses partner együttműködése a vizsgálatok során, beleértve a szükséges dokumentációk, forráskódok, technikai információk és szakértői támogatás rendelkezésre bocsátását;

- a vizsgálatok során feltárt, a fejlesztéshez kapcsolódó biztonsági megállapítások kezelése és a szükséges javító intézkedések végrehajtása.

2.12. A hozzáférés-felügyelettel kapcsolatos üzleti követelmények

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

2.13. Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz

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

A hozzáférés kizárólag az adott feladat ellátásához szükséges mértékben és időtartamra adható meg, a felhasználót bejelentkezéskor mindig azonosítani és hitelesíteni szükséges a hálózati hozzáférés biztosítása előtt.

Az FGSZ Zrt. rendszereihez vagy adataihoz kapcsolódó hálózati kommunikáció során kizárólag korszerű, biztonságos és titkosított protokollok alkalmazhatók. Elavult, nem titkosított vagy gyenge kriptográfiai megoldások alkalmazása tilos.

2.14. 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.

2.15. Naplózás és megfigyelés

FGSZ Zrt. partnerei kötelesek minden, az FGSZ Zrt. informatikai rendszereit, adatait vagy szolgáltatásait érintő tevékenység naplózásáról gondoskodni, függetlenül attól, hogy a tevékenység az FGSZ Zrt. vagy a partner informatikai rendszereiben, illetve egyéb informatikai környezetében kerül végrehajtásra. A partner köteles a naplóállományok mentését a saját mentési rendjének részeként biztosítani, valamint gondoskodni azok megfelelő megőrzéséről. A naplóállományokat védeni kell az illetéktelen hozzáféréssel, módosítással és törléssel szemben.

3. MELLÉKLETEK

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