BM ORSZÁGOS KATASZTRÓFAVÉDELMI FŐIGAZGATÓSÁG
KRITIKUS INFRASTRUKTÚRA KOORDINÁCIÓS FŐOSZTÁLY

SEGÉDLET AZ INFORMÁCIÓBIZTONSÁGI ADATSZOLGÁLTATÁS ELKÉSZÍTÉSÉHEZ ÉS BENYÚJTÁSÁHOZ

Feladatok, határidők

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 21. § (1) bekezdés alapján a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) elektronikus információbiztonsági hatósága (a továbbiakban: hatóság) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatósági nyilvántartásra vonatkozó szabályai szerinti nyilvántartást vezet. Az Ibtv. 15. § (1) bekezdés alapján a hatóság a hatáskörébe tartozó szervezetekről és azok elektronikus információs rendszereiről a következő adatokat tartja nyilván:

a) a szervezet azonosításához szükséges adatokat,

b) a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,

c) a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, a 13. § (8) bekezdésében meghatározott végzettségét,

d) a szervezet informatikai biztonsági szabályzatát,

e) a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott értesítéseket.

Fentiek megküldése a szervezetek feladata[1] és ezek végrehajtására a jogszabály határidőket szabott[2]. A kijelölő határozat véglegessé válásától számított **60 napon belül a szervezetnek be kell jelentkeznie az információbiztonsági hatóságnál, megadva a szervezet azonosításához szükséges adatokat, valamint a szervezet elektronikus információs rendszereinek biztonságáért felelős személyt kell kineveznie**, és a jogszabályban[3] előírt adatait megküldeni. Következő lépésként **90 napon belül meg kell küldeni a hatóságnak a szervezet informatikai biztonsági szabályzatát**. A harmadik nagy lépés megtételére a kijelölő határozat jogerőre emelkedésétől egy év áll rendelkezésre, ez alatt az idő alatt a szervezetnek **fel kell mérnie az Ibtv. hatálya alá tartozó[4] elektronikus információs rendszereit** és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos

[1] Ibtv. 15. § (3)
[2] Ibtv. 26. § (6) c)
[3] Ibtv. 15. § (1) c)
[4] Ibtv. 2. § (2) c)

információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: 41/2015. BM rendelet) alapján **azokat biztonsági osztályba kell sorolni, valamint meg kell állapítani a szervezet biztonsági szintjét**.

Az Ibtv. 4. § szerint: *Az elektronikus információs rendszerekre és eszközökre, szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat a hatóság az eljárása során figyelembe veszi.*

Fentiek alapján, amennyiben a szervezet auditáltatta magát az informatikai biztonságirányítási rendszerről szóló nemzetközi ISO/IEC 27001 szabvány szerint, illetve a nemzetközi egyezménnyel elfogadott Common Criteria, vagy a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma szerint minősített informatikai eszközöket, vagy más szabványok vagy ajánlások alapján tanúsított rendszerelemeket használ, ezek a minősítések garanciát szolgáltatnak a tudatos eljárásokra, így ezen tanúsítványokat a hatóság az eljárása során figyelembe veszi.

Az Ibtv. 22/A. § szerint az adatszolgáltatási kötelezettség teljesítése a hatóság által biztosított rendszerben elektronikus úton történhet, mely a következő helyen érhető el: https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet

Amennyiben technikai okokból nem küldhető elektronikus úton bejelentés, kérelem vagy adatszolgáltatás, joghatás kiváltására alkalmas ügyféli nyilatkozatot, adatközlést kizárólag személyesen benyújtva vagy postai úton – tértivevényes küldeményként – küldött iratként tudunk befogadni, melyet az alábbi címre kell eljutatni:

BM Országos Katasztrófavédelmi Főigazgatóság
Kritikus Infrastruktúra Koordinációs Főosztály
1149 Budapest, Mogyoródi út 43.

Ebben az esetben az adatszolgáltatást az átirathoz csatolt adathordozó kísérőlappal (1. számú melléklet) együtt, optikai adathordozón (CD/DVD) kérjük teljesíteni.

A szervezet bejelentése és az elektronikus információs rendszer biztonságáért felelős személy kijelölése

A szervezet a hatósághoz történő bejelentkezéshez megküldi az Ibtv. 15. § a) pont szerinti adatait, amihez a https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet linken található [BMOKFKIKFO_REG] Egyszerűsített regisztrációs űrlap „Bejelentő” fülének kitöltése szükséges.

A jogszabályi előírások[5] alapján meg kell küldeni az elektronikus információs rendszer biztonságáért felelős személy természetes személyazonosító adatait (a családi és utóneve, születési családi és utóneve, születési helye, születési ideje és anyja születési családi és utóneve), telefon- telefax számát, e-mail címét és végzettségét. Az elektronikus információs rendszer biztonságáért felelős személy kijelölésére vonatkozó feltételeket az Ibtv. 13. § (8)-(10) bekezdések és a 26/2013. (X. 21.) KIM rendelet 7. § részletezik.

[5] Ibtv. 15. § (1) c)

Az elektronikus információs rendszer biztonságáért felelős személy adatainak bejelentéséhez a https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet linken található [BMOKFKIKFO_REG] Egyszerűsített regisztrációs űrlap „Bejelentő" és Felelős" fület kell kitölteni és megküldeni. Amennyiben a szervezet regisztrálása már előzetesen megtörtént (pl. felelős személy változását szeretnék bejelenteni), úgy a „Bejelentő" fülön elegendő csak az 1.1. és 1.2. pontoknál kért adatokat megadni.

Informatikai biztonsági szabályzat megküldése

A szervezetnek rendelkeznie kell informatikai biztonsági szabályzattal, melynek elkészítésénél javasolt figyelembe venni az erre vonatkozó nemzetközi és hazai szabványokat, ajánlásokat. A szabályzatot, valamint további dokumentumokat a https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet linken található [BMOKFKIKFO_DOK] Dokumentumleíró űrlap használatával lehet megküldeni.

Az űrlappal egyidejűleg több dokumentumot lehet beküldeni. Első lépésként ki kell tölteni a beküldő szervezet azonosító adatait, kiválasztani a beküldendő dokumentum/ok típusát. A név szerint felsoroltakon kívül lehetőség van más dokumentumok, iratok benyújtására, ekkor az egyéb mezőnél kell beírni a megnevezést. Ki kell tölteni a dokumentumra vonatkozó további jellemzőket (ha értelmezhető), úgymint kiadás dátuma, dokumentum verziószáma, iktatószáma, hitelesítés módja. Amennyiben a beküldött dokumentumot valamilyen szervezetszabályozó eszköz lépteti hatályba, ennek az adatait is fel kell tüntetni (pl. az informatikai biztonsági szabályzat egy főigazgatói utasítás mellékleteként lép hatályba). Több dokumentum egyidejű beküldésénél azokat egy fájlba tömörítve lehet az űrlaphoz csatolni.

Az elektronikus információs rendszerek biztonsági osztályba sorolása

Ibtv. 7. § (1) Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az ***elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából****.*

A kijelölt létfontosságú rendszerek és létesítmények elektronikus információs rendszerei az Ibtv. hatálya alá tartoznak[6].

Az osztályba és szintbe sorolás részletes szabályait az Ibtv.-ben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. BM rendelet tartalmazza. A rendszer biztonsági osztályba sorolását kockázatelemzés alapján kell végrehajtani. A jogszabály lehetővé teszi a besorolás saját kockázatelemzési módszertan alapján történő elkészítését[7]. Amennyiben a szervezet több elektronikus információs rendszerrel (pl. ipari irányító rendszer, üzleti informatikai rendszer, irodai informatikai rendszer stb.) rendelkezik, úgy az osztályba sorolást külön-külön mindegyikre el kell végezni.

A rendszerek osztályba sorolása ötfokozatú skálán történik, a rendszer funkciói és a kezelt adatok fajtájától függően kell a bizalmasság, a sértetlenség és a rendelkezésre állás szerinti követelményeket súlyozni. Az 1-től 5-ig terjedő fokozatokhoz emelkedő irányban egyre

[6] Ibtv. 2. § (2) c)
[7] 41/2015. BM rend. 1. melléklet 1.2.

szigorodó védelmi intézkedések tartoznak, amiket az adott elektronikus információs rendszerre vonatkozóan meg kell valósítani.

A bizalmasság az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk mértékéig ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A bizalmasság elsődlegesen a (különleges) személyes-, és üzleti adatokat kezelő rendszereknél lehet fontos, tehát minden olyan esetben, ahol nem szeretnénk, ha az információ illetéktelen kezekbe kerülne.

Az sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. A sértetlenség olyan rendszereknél lehet vezető szempont, ahol fontos, hogy a kezelt adatokat illetéktelenül senki ne változtathassa meg, pl. közhiteles nyilvántartások, de termelési környezetből is említhetők a különböző mérő-, érzékelő rendszerek.

A rendelkezésre állás az adat, illetve az elektronikus információs rendszer elemeinek olyan állapota, amelyben az az arra jogosultak által a szükséges időben és időtartamra használható. Azoknál a rendszereknél, ahol alapvető igény a működés fenntartása, pl. a létfontosságú termelő, szolgáltató rendszerek, a rendelkezésre állás esik nagy súllyal latba.

A rendszerek osztályba sorolása két részből áll, az első fázisban azt kell megállapítani, hogy az adott elektronikus információs rendszer a kockázatelemzés alapján melyik biztonsági osztályba tartozik (elvárt/tervezett biztonsági osztály). A biztonsági osztályok megállapítása a káresemények szempontjából[8] a rendszer által kezelt adatok sérülésének és az ebből fakadó következmények, a szervezettel szembeni bizalomvesztés, illetve a közvetlen- és közvetett anyagi kár mértékének szintezésével történik. A jogszabályban megadott elvek szerinti besorolás alkalmazása nem kötelező, de más módszer használatánál is fel kell tüntetni az értékelési szempontokat.

A biztonsági osztályokhoz különböző szintű védelmi intézkedések vannak előírva, amiket a rendszereknek (bizonyos esetekben a szervezetnek) teljesíteniük kell. A legalacsonyabb, egyes biztonsági osztályhoz tartoznak a legenyhébb követelmények, amik az osztály számának emelkedésével egyre szigorodnak. A biztonsági intézkedések három csoportra vannak osztva. Az adminisztratív intézkedések túlnyomó többsége a szervezet tekintetében értelmezhető, a rendszer működési környezetének szabályozottságára vonatkozó követelményeket tartalmaz. Az adminisztratív intézkedések körében kerülnek felsorolásra a személyi biztonsággal kapcsolatos követelmények is. A fizikai védelmi intézkedések az elektronikus információs rendszer szempontjából érintett helyiségekre és létesítményekre, továbbá a rendszer kézzelfogható elemeire terjednek ki, ezek fizikai védelmével (biztonságtechnika, tűzvédelem, elhelyezés, javítás, karbantartás, rendszerhez és az elemeihez történő hozzáférés) kapcsolatos követelményeket tartalmaznak. A harmadik csoportba a logikai védelmi intézkedések tartoznak, amelyek a rendszer információtechnológiai eszközökkel és eljárásokkal történő védelmét takarja. Ebben az esetben a követelmények a három alapelv szerint (bizalmasság, sértetlenség, rendelkezésre állás) szerinti osztályoknál különbözőképpen érvényesülnek.

[8] 41/2015. BM rend. 1. melléklet 2.

Az osztályba sorolás második lépéseként azt kell megvizsgálni, hogy az elvárt osztályhoz előírt védelmi intézkedések hogyan teljesülnek az adott rendszer tekintetében, ez lesz a rendszer teljesített biztonsági osztálya. Azokban az esetekben, ahol a rendszer aktuális védelmének erőssége egy alacsonyabb biztonsági osztálynak felel meg, úgy a hiányosságok megszüntetésére az osztályba sorolás vezetői jóváhagyását követő 90 napon belül cselekvési tervet kell készíteni[9]. A cselekvési terv tartalmazza a feltárt hiányosságok, eltérések mellett a tervezett intézkedések felsorolását, a megvalósítására kitűzött határidőket, továbbá a felelősségi köröket.

A jogszabály lehetőséget ad a hiányosságok fokozatos megszüntetésére[10], a teljesített biztonsági osztálytól a tervezett eléréséig minden egyes következő / magasabb biztonsági osztály követelményeinek teljesítésére két év áll rendelkezésre. (A gyakorlatban: ha a rendszer elvárt biztonsági osztálya 4-es, de jelenleg csak a 2-es osztályhoz tartozó követelményeket teljesíti, úgy két éven belül kell elérnie a 3-as szintet, és újabb két éve van a 4-es szinthez tartozó követelmények kivitelezésére.)

A rendszerek osztályba sorolásának elvégzéséhez az OKFovi4602 nevű Excel fájl nyújt segítséget, ami a https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet helyem érhető el. A munkafüzetet minden egyes elektronikus információs rendszerre külön-külön kell elkészíteni.

A munkát a táblázat „Összegzés” munkalap fejlécének kitöltésével célszerű kezdeni, a szervezet és a rendszer azonosításához szükséges adatok kitöltésével, több rendszer esetén ezzel elkerülhető az adatok keveredése. Következő lépésként az „Osztályba sorolás” megnevezésű munkalapon, vagy az ajánlott kritériumok vagy saját módszertan alapján kell meghatározni mindhárom alapelv szerint az elvárt biztonsági osztályt. Ha az ajánlott módszert választja, akkor a felsorolt kérdéseket kell megválaszolni a három biztonsági cél sérülése tekintetében. Saját módszertan használatánál a besorolási szempontokat, vagy a módszertan leírását tartalmazó dokumentum hivatkozását „A fentiektől eltérő szempont szerint történt az osztályba sorolás” rész alatti szöveges mezőben lehet rögzíteni, és itt kell megadni a három biztonsági cél szerinti besorolást is. Bármelyik módszer alkalmazásánál a bizalmasság, sértetlenség, rendelkezésre állás megállapított osztálya automatikusan megjelenik az „Összegzés” munkalapon, és az adott rendszer biztonsági osztálya a három alapelv szerinti osztályok közül a legmagasabb lesz.

Miután meghatároztuk a rendszer biztonsági osztályát, a 41/2015. BM rendelet védelmi intézkedések katalógusában alkalmazott számozás alapján jelölt „3.1.1.” – „3.3.13.” munkalapokon jelölni kell, hogy a rendszer teljesíti-e az adott részkövetelményt. A táblázat automatikusan jelzi, hogy a meghatározott osztálynál kötelező-e az adott követelmény teljesítése (0, N: nem kötelező, X, K: kötelező). Az itt felvitt adatok alapján az „Összegzés” munkalapra automatikusan átvezetődik, hogy a rendszer teljesíti-e a meghatározott osztályhoz tartozó követelményeket.

A meg nem valósult intézkedéseknél a táblázatban lehetőség van jelölni a cselekvési tervnek megfelelően a megvalósítandó intézkedések bevezetésének tervezett, illetve a megvalósítás tényleges dátumát, valamint a tervezéshez, illetve a bevezetéshez kapcsolódó dokumentumok adatait, ami a későbbi ellenőrzéseknél nyújt nagy segítséget.

[9] Ibtv. 8. § (5)
[10] Ibtv. 8. § (3)

A jogszabály bizonyos esetekben eltérést engedélyez az előírt védelmi intézkedések megvalósítása alól. A fizikai és adminisztratív védelmi intézkedéseket abban az esetben szükséges alkalmazni, ha az értelmezhető az elektronikus információs rendszerre és környezetére, beleértve a használó személyeket és a környezeti infrastruktúrát is. Továbbá a biztonsági követelményeket csak akkor kell teljesíteni, ha a rendszer használja az intézkedésben feltüntetett technológiát, valamint csak a rendszer azon komponenseire, amelyek a csökkenteni kívánt kockázat tekintetében relevánsak. A kizárólag egyedüli biztonsági célhoz (bizalmasság, sértetlenség, rendelkezésre állás) tartozó biztonsági intézkedés esetében bizonyos körülmények esetén szintén lehetőség van az eltérésre.

Bizonyos esetekben lehetőség nyílik helyettesítő intézkedések alkalmazására, amennyiben azok az eredetivel egyenértékű védelmet nyújtanak az adott fenyegetésekkel szemben.

Az szervezet biztonsági szintbe sorolása

Ibtv. 9. § (1) A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében ***a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni*** *a jogszabályban meghatározott szempontok szerint.*

Az elektronikus információs rendszerrel rendelkező szervezet/szervezeti egység biztonsági szintjének meghatározása a szervezet információbiztonsági menedzsmentjének fejlettségét, érettségét méri. A biztonsági osztályokhoz hasonlóan szintén ötfokozatú rendszerben a leggyengébb szint azt jelenti, hogy a szervezetnél vannak az információbiztonságot érintő szabályozók, de a folyamatok ad hoc jellegűek, nem ellenőrzöttek. A szintek emelkedésével párhuzamosan a folyamatok szabályozottabbak, dokumentáltak, ellenőrzöttek, számon kérhetőek, oktatottak, teszteltek, mérhetőek, auditáltak lesznek. A szervezet elektronikus információs rendszereinek biztonsági osztálya és a szervezet biztonsági szintje között célszerű erős kapcsolatot tartani, mert belátható, hogy szigorú védelmi intézkedéseket csak fejlett biztonsági kultúrával rendelkező szervezet tud megbízható módon végrehajtatni, míg az ellenkező oldalon, az alacsony biztonsági követelményeket támasztó rendszerek használatához nem szükséges sok anyagi- és humán erőforrást használó biztonsági menedzsment fenntartása.

Amennyiben léteznek, célszerű végrehajtani az elektronikus információs rendszerek üzemeltetését, fejlesztését végző, vagy az üzemeltetésért, illetve az információbiztonságért felelős szervezeti egységek biztonsági szintbe sorolását is. A biztonsági szintet az elektronikus információs rendszer felhasználásának módja határozza meg, tehát a megállapított értékek különbözhetnek a szervezet egészének és a fenti, speciális szervezeti egységeknek a tekintetében. Ennek eredményeképpen a magasabb biztonsággal védendő szervezeti egységek szintbe sorolása elválik a szervezet biztonsági szintjétől, tehát attól, hogy egy szervezeten belül információbiztonsági szempontból magasabb védelmi szinten lévő szervezeti egység működik, nem kell a teljes szervezetre a magasabb elvárásokat megvalósítani, így jelentős költség takarítható meg.

A 41/2015. BM rendelet 2. mellékletében felsorolt követelmények alapján meg kell vizsgálni a szervezet aktuális biztonsági szintjét. Amennyiben a szervezet nem teljesíti a tervezett biztonsági szinthez meghatározott követelményeket, úgy a biztonsági osztálynál leírtakhoz hasonló módon cselekvési tervet kell készíteni, azzal az eltéréssel, hogy ha a szervezet nem éri el az 1-es biztonsági szintet, abban az esetben 8 év áll rendelkezésére az első lépcsőfok teljesítésére.

A szintbe sorolás adatait a https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet linken elérhető OKFszvi200 Excel fájlban kell rögzíteni.

Külön munkafüzetet kell kitölteni minden besorolandó szervezeti egységre és a szervezetre, ezek megnevezését és típusát (az általános jelenti magát a szervezetet) az „Összegzés" fül fejlécében kell feltüntetni. A táblázat kitöltését a „Szintbe sorolás" munkalapon célszerű kezdeni az eldöntendő kérdések megválaszolásával, ami automatikusan generálja az elvárt szint értékét az „Összegzés" fülön. Következő lépésként a „Követelmények" munkalapon meg kell vizsgálni, hogy a megállapított biztonsági szinthez tartozó követelményeket teljesíti-e az adott szervezet/ szervezeti egység. Az osztályba soroláshoz hasonlóan a táblázat eltérő színnel jelzi a kötelezően megvalósítandó intézkedéseket.

A nem teljesített kötelező követelmények megvalósításának ütemezésére cselekvési tervet kell készíteni. Ehhez nyújt segítséget a munkalap „Tervezés" és „Megvalósítás" része, ahol dokumentálni lehet az adott követelményhez tartozó határidőket, valamint a kapcsolódó dokumentumok (tervezési dokumentum, intézkedést bevezető, elrendelő dokumentum stb.) paramétereit. A „Tervezés" részből készített kivonat segítséget nyújthat a cselekvési terv összeállításához.

A „Követelmények" fül kitöltése után az „Összegzés" fülön megjelenik a vizsgált elem teljesített biztonsági szintje, valamint összefoglaló adat az egyes szintekhez tartozó követelmények megvalósulásáról és a kapcsolódó dátumokról.

A biztonsági szintbe sorolásánál a 41/2015. BM rendelet 2. melléklet 5. pontja *a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység* számára automatikus jelleggel az 5-ös szintet írja elő. Az Ibtv. 9. § (6) bekezdése alapján a létfontosságú rendszerek, létesítmények tekintetében az irányadó besorolástól el lehet térni Ennek a hatóság általi elfogadásához a szervezetnek a kockázatokra kiterjedő indoklással ellátott kérelmet kell a hatósághoz benyújtani. A kérelemnek arra kell irányulnia, hogy a hatóság fogadja el a szervezet alacsonyabb szintű besorolását. A kérelemhez meg kell adni, hogy a besorolt szervezet, illetve önállóan besorolt szervezeti egységek milyen szintértéket kaptak. Csatolni szükséges egy részletes leírást a szervezetről illetve az önállóan besorolt szervezeti egységekről, valamint a szervezet által használt elektronikus információs rendszerekről. A kérelemben szükséges megjelölni, hogy milyen szintértéket javasol a szervezet vezetője, ennek alátámasztására részletes, a kockázatokra kitérő indokolást is az anyaghoz kell csatolni.

A hatóság a kérelmet megvizsgálva, döntésében engedélyezi vagy megtagadja az alacsonyabb szintbe sorolást. Az ügyfél által benyújtott biztonsági osztályba és szintbe sorolás mellé csatolni kell a részletes kockázatelemzést, a hatóság ezek együttes, összefüggéseiben történő vizsgálatával hozza meg végleges döntését.

Az osztályba- és szintbe sorolás adatait tartalmazó fájlokat a https://www.katasztrofavedelem.hu/34014/letfontossagu-rendszerek-es-letesitmenyek-urlapok-es-kitoltesi-segedlet linken található [BMOKFKIKFO_DOK] Dokumentumleíró űrlaphoz csatoltan lehet megküldeni.

Futtatási környezet

A [BMOKFKIKFO_REG] Egyszerűsített regisztrációs űrlap, [BMOKFKIKFO_DOK] Dokumentumleíró űrlap használatához az Általános Nyomtatványkitöltő telepítése, szükséges, melyhez legalább Java 1.6 futtatókörnyezetnek kell rendelkezésre állnia.

Az OKFovi4602 és az OKFszvi200 űrlapok MS Excel 2013 programmal teszteltek, és makróbarát Excel munkafüzet sablon formában lettek közzétéve. A kitöltésükhöz az Ön munkakörnyezetében is engedélyezni kell a makrók futtatását, ennek hiányában a munkafüzetek kisebb funkcióveszteséggel jelennek meg: nem működik a csoportosított sorok, oszlopok becsukása és kinyitása.

Problémákba ütközött?

Amennyiben a vonatkozó jogszabályok alkalmazásához, vagy az adatszolgáltatás részleteivel kapcsolatos kérdésekben további tájékoztatásra is szüksége van, – előzetes időpont-egyeztetés alapján – az Országos Katasztrófavédelmi Főigazgatóságon történő konzultáció keretében vagy a feltüntetett elérhetőségeinken a további információkat rendelkezésükre bocsátjuk.

Cím: 1149 Budapest, Mogyoródi út 43. ✉: 1903 Budapest Pf.: 314
Telefon: +36 (1) 469-4470
E-mail: kikfo@katved.gov.hu