INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az alábbi aláírások igazolják, hogy a jóváhagyók elolvasták, megértették és elfogadták a dokumentumot:

|  |  |  |  |
| --- | --- | --- | --- |
| **Név** | **Beosztás** | **Aláírás** | **Dátum** |
| **Jóváhagyó:** | ügyvezető |  |  |
| A szervezet vezetője igazolja, hogy a dokumentum megfelel a szervezet igényeinek. | | | |
| **Jóváhagyó:** | ügyvezető |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Jóváhagyás dátuma** | **Felülvizsgálati határidő** | **Adat kategória** | **Megőrzési idő** |
| 2018. május 25. | Szükség szerint | Belső - nem szabályozott | Az új verzió megjelenéséig. |

**Tartalom**

[1 Bevezetés 4](#_Toc498585397)

[1.1 A dokumentum célja 4](#_Toc498585398)

[1.2 A dokumentum szervezeti hatálya 4](#_Toc498585399)

[1.3 A dokumentum tárgyi hatálya 4](#_Toc498585400)

[1.4 A dokumentum személyi hatálya 4](#_Toc498585401)

[1.5 Kiadás dátuma, érvényessége 4](#_Toc498585402)

[1.6 Kapcsolódó dokumentumok 5](#_Toc498585403)

[2 Az információbiztonság szervezete 6](#_Toc498585404)

[2.1 Általános szabályok 6](#_Toc498585405)

[2.2 Informatikai biztonsági vezető 6](#_Toc498585406)

[2.3 Informatikai biztonsági adminisztrátor 6](#_Toc498585407)

[2.4 Adatgazdák 6](#_Toc498585408)

[2.5 Felhasználók 7](#_Toc498585409)

[2.6 Külső szolgáltatók 7](#_Toc498585410)

[2.7 Felelősség 8](#_Toc498585411)

[3 Információs rendszerek kockázatkezelése 9](#_Toc498585412)

[3.1 Kockázatelemzési alapelvek 9](#_Toc498585413)

[3.2 Kockázatelemzési eljárásrend 9](#_Toc498585414)

[3.3 Felelősség 10](#_Toc498585415)

[4 Adatosztályok 11](#_Toc498585416)

[4.1 Adatosztályozás 11](#_Toc498585417)

[4.2 Felelősség 11](#_Toc498585418)

[5 Adatkezelési eljárásrend 12](#_Toc498585419)

[5.1 Alapkövetelmények 12](#_Toc498585420)

[5.2 Adatcsere, adattovábbítás 12](#_Toc498585421)

[5.3 Hálózati határvédelem 13](#_Toc498585422)

[5.4 Hálózati adatátvitel biztonsága 13](#_Toc498585423)

[5.5 Felelősség 14](#_Toc498585424)

[6 Adatvédelmi hatásvizsgálati eljárásrend 15](#_Toc498585425)

[6.1 Alapkövetelmények 15](#_Toc498585426)

[6.2 Felelősség 15](#_Toc498585427)

[7 Jogosultságkezelés 16](#_Toc498585428)

[7.1 Az információ-hozzáférés szabályozása 16](#_Toc498585429)

[7.2 A hozzáférési jogok kezelése 16](#_Toc498585430)

[7.2.1 Igénylés 16](#_Toc498585431)

[7.2.2 Kiadás és érvényesítés 17](#_Toc498585432)

[7.2.3 Módosítás 17](#_Toc498585433)

[7.2.4 Visszavonás 17](#_Toc498585434)

[7.2.5 Ellenőrzés 18](#_Toc498585435)

[7.3 Speciális jogosultságok kezelése 18](#_Toc498585436)

[7.4 A felhasználói jelszókezelés 18](#_Toc498585437)

[7.4.1 Felhasználói felelősségek 19](#_Toc498585438)

[7.5 Felhasználói informatikai biztonsági követelmények 20](#_Toc498585439)

[7.6 Nyilvánosan hozzáférhető információk kezelése 20](#_Toc498585440)

[7.7 Távmunka és távoli elérés szabályai 20](#_Toc498585441)

[7.8 Felelősség 21](#_Toc498585442)

[8 Adatmentés 22](#_Toc498585443)

[8.1 Információk biztonsági mentése 22](#_Toc498585444)

[8.2 Mentési eljárás 22](#_Toc498585445)

[8.3 Archiválási eljárás 23](#_Toc498585446)

[8.4 Visszatöltés mentési állományból 23](#_Toc498585447)

[8.5 Felelősség 23](#_Toc498585448)

[9 Biztonsági helyzet- és eseményértékelés 24](#_Toc498585449)

[9.1 Naplózás 24](#_Toc498585450)

[9.2 Incidenskezelés 25](#_Toc498585451)

[9.2.1 Bejelentési kötelezettség 26](#_Toc498585452)

[9.2.2 Az érintett tájékoztatása az adatvédelmi incidensről 26](#_Toc498585453)

[9.3 Ügy és üzemmenet-folytonosság 27](#_Toc498585454)

[9.4 Felelősség 27](#_Toc498585455)

[10 Adatkezelési kérés- és panaszkezelés 28](#_Toc498585456)

[10.1 Alapelvek 28](#_Toc498585457)

[10.2 Az érintett jogai 28](#_Toc498585458)

[10.3 Az érintettek kéréseinek kezelése 30](#_Toc498585459)

[10.4 Felelősség 31](#_Toc498585460)

[11 Oktatás, képzés, tudatosítás 32](#_Toc498585461)

[11.1 Számítógéphasználati elvek 32](#_Toc498585462)

[11.2 Internet használata 32](#_Toc498585463)

[11.3 e-mail, elektronikus levelezés 33](#_Toc498585464)

[11.4 Közösségi média használata 34](#_Toc498585465)

[11.5 Oktatási eljárásrend 34](#_Toc498585466)

[11.6 Felelősség 35](#_Toc498585467)

[12 Ellenőrzési eljárásrend 36](#_Toc498585468)

[12.1 Általános elvek 36](#_Toc498585469)

[12.2 Az ellenőrzések területei, célkitűzései 36](#_Toc498585470)

[12.3 Felelősség 36](#_Toc498585471)

[13 Hivatkozások 37](#_Toc498585472)

[14 Dokumentum történet 37](#_Toc498585473)

# Bevezetés

Jelen dokumentum a **Firstmed-FMC Egészségügyi Szolgáltató Korlátolt Felelősségű Társaság** (székhelye: 1015 Budapest, Hattyú utca 14., cégjegyzékszáma: 01-09-958986, a továbbiakban TÁRSASÁG, vagy Társaság) informatikai biztonsági szabályzata (a továbbiakban IBSZ) az Európai Parlament és a Tanács (EU) [2016/679 rendeletében](http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=EN), a kapcsolódó jogszabályokban és szabványokban meghatározottak szerint.

## A dokumentum célja

Az IBSZ célja a TÁRSASÁG informatikai biztonsági követelményrendszerének és környezetének meghatározása, mely leírja a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait, az ehhez szükséges egyes szerepköröket és a végrehajtás gyakoriságát vagy idejét. © TMSI Kft. 2017. nov: 753951+VP7751

## A dokumentum szervezeti hatálya

Az IBSZ kiterjed a Társaság információkezeléssel és – feldolgozással kapcsolatos összes folyamatára és tevékenységére, a Társaság tulajdonában vagy használatában lévő elektronikus információs rendszerekben előforduló adatokra, továbbá a Társasággal szerződéses jogviszonyban álló valamennyi szervezetre, amelynek munkavállalói, vagy alvállalkozói a Társaság által használt rendszerekhez, illetve az azokon tárolt adatokhoz hozzáféréssel rendelkeznek. A Társaság kötelessége, hogy a szervezeteknek legyen módjuk a rájuk vonatkozó elvárások és kötelezettségek megismerésére.

Az itt nem szabályozott kérdésekben a Társaság Szervezeti és Működési Szabályzata a mérvadó.

Amennyiben a jelen dokumentum szerinti valamely pozíció betöltésére, vagy az ahhoz rendelt feladatok megfelelő felelősének meghatározására még nem került sor a Társaság szervezetében, úgy a megjelölt tisztség és az ahhoz tartozó felelősség alatt az ügyvezetőt, mint a szervezet vezetőjét kell érteni.

## A dokumentum tárgyi hatálya

Jelen dokumentum tárgyi hatálya kiterjed az informatikai eszközök elhelyezésére szolgáló létesítményekre (épületekre, telephelyekre), a Társaságnál meglévő, használatban lévő vagy a jövőben bevezetett, alkalmazott informatikai eszközre, rendszerre, a kezelt adatokra, azok környezetét alkotó rendszerelemre teljes életciklusában a tervezéstől, elkészítéstől, a rendszerből történő teljes kivonásáig, vagy megsemmisítésig.

## A dokumentum személyi hatálya

Az elfogadott IBSZ vonatkozik:

* a Társaság valamennyi alkalmazottjára,
* a Társaság összes közreműködő munkatársára,
* a Társasággal szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, vagy titoktartási nyilatkozatok alapján.

Az IBSZ személyi hatálya kiterjed a Társaság valamennyi képviselőjére, vezetőjére, a rendszerek felhasználóira, fejlesztőire, üzemeltetőire.

Ezeken kívül a dokumentum hatálya kiterjed a Társasággal külső, megbízásos (szerződéses) eseti munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a fenti szerződések tartalmának megfelelő kialakításával kell biztosítani és a biztonságért felelős személyek közreműködésével kell megvalósítani.

## Kiadás dátuma, érvényessége

Jelen szabályzat a kiadás napján lép hatályba, és mindaddig érvényesnek tekintendő, amíg annak egy új változata jóváhagyásra nem kerül.

Az IBSZ-ben előálló bármilyen változás verziószám változással jár, melyet a Dokumentum történetben fel kell vezetni, feltüntetve a verziószámot a kibocsátás napját és a változások rövid összefoglalását.

Az IBSZ írásos formában minden résztvevő számára elérhető a Társaság székhelyén, illetve elektronikus formában a Társaság merevlemezén/szerverén.

A Szabályzat, illetve mellékleteinek felülvizsgálatára az alábbiak szerint kerül sor:

* évente egy alkalommal, a belső felülvizsgálatok során,
* rendkívüli, a megváltozott körülmények hatására a felülvizsgálatot el kell végezni az alábbi események bármelyikének bekövetkezésekor:
  + a Társaság Szervezeti és Működési Szabályzata (a továbbiakban: SZMSZ) módosítása;
  + az információbiztonságot is érintő jogszabály-változás, amennyiben annak hatálya a Társaságra is kiterjed;
  + az információkezelést és –feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás;
  + a Társaság tulajdonában vagy használatában lévő elektronikus információs rendszerekben, illetve azok fizikai környezetében beálló lényeges változás.
* minden olyan esetben, amikor a Szabályzatban leírtakhoz képest egyéb jelentős változás történik.

A mindenkori felülvizsgálat végrehajtása az Informatikai felelős feladatát jelenti.

## Kapcsolódó dokumentumok

Az IBSZ elkészítéséhez felhasznált dokumentumok

* SZMSZ [1]
* Informatikai biztonsági politika [2]

# Az információbiztonság szervezete

**Cél:** A biztonsági feladatok ellátására és ellenőrzésére azonosítható szerepkörök álljanak rendelkezésre.

## Általános szabályok

A Társaság e szabályzatban megfogalmazott világos iránymutatással, elkötelezettsége kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök egyértelmű kijelölésével és elismerésével aktív módon támogatja az informatikai biztonságot a szervezeten belül.

A szerepkörökkel kapcsolatos általános – a szervezeti egység szintjén értelmezett – felelősségi szabályokat a Társaság Szervezeti és Működési Szabályzata (SZMSZ), az egyes információbiztonsági szempontból releváns folyamatokban, eljárásokban értelmezett részletes feladatokat és felelősségi szabályokat az adott felhasználó munkaköri leírása tartalmazza.

## Informatikai biztonsági vezető

A Társaság informatikai biztonsági megbízottja a szervezet informatikai referense.

Az informatikai biztonság terén feladata:

* A Társaság informatikai biztonsági feladatainak tervezése, meghatározása, irányítása és ellenőrzése.
* Az informatikai biztonsági szabályzatok elkészítése, vagy azokban való közreműködés, a szabályzatok betartatása, a vonatkozó részeinek karbantartása.
* Részvétel a biztonsági események felderítésében, elemzésében és kezelésében.
* Az információbiztonsági tevékenység koordinálása.
* Az adat- és információvédelemmel kapcsolatos veszélyforrások felmérése és elemzése.
* Gondoskodás az informatikai biztonsági szabályzatok naprakészen tartásáról, az abban foglaltak betartásának ellenőrzéséről.
* Az informatikai biztonsági eszközök állapotának figyelemmel kísérése, javaslatot azok cseréjére, bővítésére.
* Az informatikai biztonságra vonatkozó oktatás megszervezi és lebonyolítása.

## Informatikai biztonsági adminisztrátor

Az informatikai biztonsági feladatok technológiai szintű ellátását az informatikai biztonsági adminisztrátorok (pl. vírusvédelmi felelős megbízott, rendszerüzemeltető megbízott) látják el. Ezt a szerepkört egy vagy több személy töltheti be, akiket az Informatikai biztonsági vezető javasol. Az informatikai biztonsági adminisztrátorok feladata a szabályzatokban, utasításokban szereplő jogosultsági és informatikai biztonsági feladatok technológiai megvalósítása az egyes elektronikus információs rendszereken, eszközökön.

## Adatgazdák

Az adatgazdai megbízotti intézmény célja a Társaság adatvagyona számára a megfelelő biztonsági környezet kialakítása azáltal, hogy az adatok kezelésének szabályaival kapcsolatos felelősségek az adatokat ténylegesen felhasználó üzleti folyamatokra, szervezeti egységekre hárulnak.

A Társaság egyes folyamatai, szervezeti egységei nevében, az általuk használt adatok vonatkozásában az adatgazdák állapítják meg az adatkezelés biztonsági követelményeit az informatikai biztonsági vezető segítségével és együttműködésével. Az egyes adatokhoz, adatbázisokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát az érintett adatok adatgazdái határozzák meg.

Az adatgazdák feladata, hogy a felelősségi körükbe tartozó adatok vonatkozásában megjelenési formájuktól függetlenül az adatok be- vagy átsorolását elvégezzék a különböző biztonsági osztályokba.

Az adatgazda a besorolásról írásban tájékoztatja az Informatikai csoportot. Az Informatikai csoport a besorolást átvezeti az általa vezetett adatosztályozási séma nyilvántartásában, továbbá – amennyiben szükséges – kezdeményezi a besorolásnak megfelelő jelzés feltüntetését az adat nyomtatott megjelenési formáin.

Az adatgazdai teendők ellátása a Társaság a felelőssége, aki az adatgazdai tevékenységek ellátásával mást is megbízhat.

## Felhasználók

**Felhasználó:** a Társaság összes, elektronikus információs rendszert használó munkatársa/megbízottja.

**Speciális felhasználó:** adminisztrátori, root, stb. speciális jogosultsággal rendelkező felhasználók. Minden adminisztrátor egy felhasználó is egyben, csak egy speciális fiók abban a tekintetben, hogy ő teljes joggal rendelkezik az adott rendszer felett.

**Külső felhasználó:** a Társasággal kapcsolatban álló külső felek a Társaság biztonsági szabályainak és elvárásainak betartása mellett férhetnek hozzá a Társaság elektronikus információs rendszeréhez.

A külső felhasználók hozzáférését a hozzáférés indokának megszűnte után azonnal, ill. az együttműködés lejártakor automatikusan meg kell szüntetni.

## Külső szolgáltatók

A külső szolgáltatók és együttműködő partnerek igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kikötni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a Társaság számára az ellenőrzés feltételeit.

Minden érintett szereplővel titoktartási nyilatkozatot kell kitöltetni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza.

A nyilatkozatnak tartalmaznia kell a titoktartás tárgyi hatályát, mely szerint milyen információk tartoznak védett információk közé, illetve melyek a minősített esetek (különösen védett információ kategóriák). A hatályos jogszabályoknak megfelelően a titoktartási kötelezettség megszegésért kártérítési kötelezettséget kell megállapítani.

A Társaság éles, üzemi rendszereiből származó adatokat csak tesztelési célból és csak anonimizálva lehet átadni külső szolgáltatónak.

A külső felekkel kötött megállapodásoknak vagy szerződéseknek pontosan tartalmazniuk kell:

* a megállapodásban részt vevő felek kölcsönös kötelezettségét,
* a joganyagokra vonatkozó felelősséget, pl. adatvédelmi jogszabályok kérdésében,
* szellemi tulajdonjogokat és a szerzői jog átruházását, valamint az együttes csoportmunka védelmét,
* a tevékenységük pontos meghatározását,
* a hozzáférési jogosultságaikat,
* a hozzáférés módját, idejét és korlátait, különös tekintettel a helyszíni munkavégzésre
* a Társaság biztonsági előírásainak- és kontrolljainak elfogadását,
* a titoktartási nyilatkozataikat,
* az ellenőrzés feltételeit, valamint az ezekről szóló jelentések meghatározását,
* a szerződésben lefektetett felelősségek auditálásának jogát, vagy az auditok további külső féllel történő elvégeztetésének jogát,
* a karbantartás és rendszerkövetés kérdéseit
* a problémamegoldás folyamatát – ha lehetséges – az előre nem látható események figyelembevételével,
* a biztonsági eseményekről és a biztonság megsértéséről szóló jelentések, értesítések és kivizsgálások esetére vonatkozó intézkedéseket,
* a szerződés teljesítésébe további alvállalkozók bevonásának feltételeit, titoktartásra vonatkozó megállapodásokat.

Külső felek szolgáltatásaival kapcsolatos változásoknál biztosítani kell, hogy a változásokat csak a megfelelő jogosultságokkal lehessen kezdeményezni, és a végrehajtás ellenőrzött és dokumentált körülmények között történjen az igény felvetésétől az átadás-átvételig.

A külső szolgáltatókkal kötött szerződésekben szabályozni kell a változáskezelési eljárásokat a külső fél által nyújtott szolgáltatásokra, melyek a következőket biztosítják:

* a változások végrehajtása csak a megfelelő jóváhagyás után történjen,
* a végrehajtás során is érvényesüljenek a biztonsági előírások- és kontrollok,
* az átvétel során ellenőrzésre kerüljön a specifikációban/változási kérelemben leírtak teljesülése.

A külső szolgáltatóktól elvárt védelmi intézkedéseket a Társaság informatikai csoportja legalább évente ellenőrzi.

Minden harmadik féllel kötött megállapodás esetében rögzíteni kell a jelen Szabályzat által meghatározott biztonsági követelményeket.

## Felelősség

Az információbiztonság szervezetével kapcsolatos felelősség a Társaságot (vagy ha van, úgy az általa kijelölt felelős vezetőt) terheli.

# Információs rendszerek kockázatkezelése

**Cél**: Annak biztosítása, hogy azonosíthatóak legyenek a tényleges informatikai fenyegetések, illetve, hogy a Társaságnak információt szolgáltasson az információbiztonsággal kapcsolatos döntések meghozatalához, az információbiztonsági célok megvalósulásához.

## Kockázatelemzési alapelvek

A Társaságszámára az informális, alapszintű kockázatkezelés képezi az alapját az információbiztonsági védelmi intézkedések kiválasztásának.

Az informatikai kockázatelemzésnek illeszkednie kell a Társaságteljeskörű kockázatelemzéséhez.

Az információbiztonsági kockázatok körébe tartozik az információs rendszerek tervezési, szervezési, fejlesztési, megvalósítási, üzemeltetési és monitorozási folyamataiban fellelhető minden olyan körülmény, amely az információbiztonsági követelmények (bizalmasság, sértetlenség, hitelesség, funkcionalitás, rendelkezésre állás) bármelyikének nem-teljesülésével fenyeget.

A kockázatelemzés során

* azonosítani kell a fenyegetéseket,
* értékelni kell a sérülékenységet, a sebezhető pontokat,
* értékelni kell a sebezhetőségek előfordulásának valószínűségét,
* meg kell becsülni a várható hatásokat.
* meg kell határozni az adott kockázatokhoz használt analizálás módszerét, amely lehet
  + mennyiségi
  + minőségi
  + vagy mennyiségi és minőségi

A [2013. évi L. törvény](http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.338522) az állami és önkormányzati szervek elektronikus információbiztonságáról egyik kapcsolódó joganyaga a 41/2015. (VII. 15.) BM rendelet, amely a kockázatkezelésről a következőképpen rendelkezik: „Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.”

Bár a Társaság nem tartozik e törvény, illetve BM rendelet hatálya alá, a kockázatelemzés szempontjából mégis ezt a jelzett módszertant ([„Osztályba sorolás és védelmi intézkedés űrlap”](http://neih.gov.hu/urlapok)), mint elfogadott hazai keretrendszert kívánja alkalmazni.

## Kockázatelemzési eljárásrend

A Társaságban háromévente egyszer, vagy szükség esetén soron kívül, dokumentált módon, az informatikai biztonsági vezető vezetésével felül kell vizsgálni az információbiztonsági kockázatelemzést.

A kockázatelemzési folyamatban az Informatikai csoport delegált munkatársai, valamint az elemzett területek, folyamatok képviselői vesznek rész.

A Társaságinformatikai kockázatbecslése az alábbi lépésekből áll:

* A rendszer leírása
* A veszélyek meghatározása (emberi, természeti, környezeti)
* A sebezhetőségek elemzése
* Az óvintézkedések elemzése (technikai, üzemeltetési, menedzsment)
* A valószínűségek meghatározása (magas, közepes, alacsony)
* Hatáselemzés (kritikus, súlyos, mérsékelt, kismértékű)
* A kockázati szint meghatározása (alacsony, mérsékelt, magas, kritikus)
* Javaslat óvintézkedésekre
* Az eredmények dokumentálása

A kockázatelemzések eredményét kockázatelemzési jelentésben kell rögzíteni és a Társaságban bevált gyakorlat szerint kell gondoskodni arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

A kockázatok ismeretében meg kell határozni az elhárításhoz szükséges feladatokat és a kapcsolódó felelősségi köröket, erőforrásokat.

A kockázatértékelésnek tartalmaznia kell egy kockázati cselekvési tervet, amelynek célja, hogy költséghatékony ellenőrzési és biztonsági intézkedésekkel folyamatosan alacsony szinten tartsa a Társaságkitettségét az informatikai fenyegetettségeknek.

A kockázatok értékelése során meg kell határozni a Társaságkockázatviselési képességét, vagyis azt a kockázati szintet, amelynél magasabb információbiztonsági kockázatot a Társaságnem vállalhat.

A kockázatértékelés keretében a kockázatok feltárása és mérése, a szervezeti célkitűzések, a kockázatbecslési eljárásban rejlő bizonytalanságok, valamint a biztonsági és ellenőrzési intézkedések költségeinek függvényében meg kell határozni az elfogadható kockázat szintjét.

## Felelősség

A kockázatkezelés irányítása az ügyvezető (vagy ha van, úgy az általa kijelölt felelős vezető(t)) felelőssége.

# Adatosztályok

## Adatosztályozás

A Társaságinformációrendszerében feldolgozott, továbbított, tárolt adatok kockázatarányos védelmének biztosítása érdekében az adatokat is be kell sorolni biztonsági osztályokba.

Az információrendszerekben elektronikusan tárolt adatok esetén az adatok azon halmazát, amelyekre a tárolás számítástechnikai körülményeiből adódóan jellemzően azonos védettség valósítható meg (közös adatbázis, azonos könyvtár), ugyanabba a biztonsági osztályba kell sorolni, mégpedig oly módon, hogy a halmaz egészére ki kell terjeszteni a halmaz legérzékenyebb elemének besorolását.

Az adatosztályozás során az adatokat szintén a kockázatelemzés eredményei alapján kell besorolni alacsony, mérsékelt, magas, kritikus osztályokba.

Alapelv és kiinduló állapot, hogy a rendszerekben kezelt adatok biztonsági osztálya megfelel az őket kezelő elektronikus információs rendszer biztonsági osztályának.

Az adatgazdák – az informatikai biztonsági vezető közreműködésével – az adatok osztályozását felülvizsgálják, és a besorolást megváltoztathatják vagy jóváhagyhatják

1. ha az információkezelést és –feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében lényeges változás áll be;
2. a Társaságtulajdonában vagy használatában lévő elektronikus információs rendszerekben lényeges változás áll be.

## Felelősség

Az adatok osztályozását az ügyvezető (vagy ha van, úgy az általa kijelölt felelős vezető(t)) koordinálja.

# Adatkezelési eljárásrend

**Cél:** Biztosítani, hogy a Társaságelektronikus információs rendszere konzisztens legyen az adatkezelés területén abban, hogy az elvárt eredményt hozza az elvárt teljesítmény mellett.

## Alapkövetelmények

A Társaságelektronikus információs rendszereiben tárolt és feldolgozott adatok vonatkozásában az egyes ügyviteli és üzemeltetési folyamatok eljárási szabályaiban gondoskodni kell arról, hogy az adatok sértetlensége az adatkezelés során megőrződjön.

Az adatosztályozási fejezet szerinti magas vagy kritikus biztonsági osztályba sorolt adatokat:

1. a bevitel után titkosítottan kell tárolni, kezelni vagy továbbítani,
2. külső adatátviteli csatornák használata során meg kell győződni arról, hogy az átvitel során nem történt adatmódosulás, illetve
3. hogy az átvitel megtörtént.

Információbiztonsági szempontból az adat-előkészítési folyamatok ügyviteli szabályainak:

1. gondoskodniuk kell az adatrögzítést megelőző megfelelő jóváhagyási eljárásról;
2. biztosítaniuk kell a munkaállomás és a felhasználó egyértelmű azonosítását és gondoskodniuk kell azok folyamatos használatáról;
3. biztosítaniuk kell a rögzített adat és a forrásdokumentum közötti kapcsolat (iktatószám, vagy más alkalmas egyedi azonosító) rögzítését;
4. biztosítaniuk kell az adatok teljes körűségét, pontosságát és érvényességét;
5. biztosítaniuk kell, hogy a jóváhagyott adatok teljes körűsége, pontossága és érvényessége az előkészítés további szakaszaiban is fennáll;
6. tartalmazniuk kell a hibásnak minősülő forrásdokumentumok kezelésének eljárásait;
7. tartalmazniuk kell a hibásan rögzített adatokkal kapcsolatos javítási és eszkalációs (problémamegoldó, menedzselő) eljárásokat;
8. tartalmazniuk kell az egyes forrásdokumentumok biztonsági osztályainak megfelelő követelmények teljesítésének módját.

Az adatfeldolgozást végző alkalmazásoknak tartalmazniuk kell a hibák megelőzését, felfedezését és korrigálását szolgáló funkciókat.

Az adatfeldolgozási folyamatok ügyviteli és informatikai üzemeltetési szabályainak:

1. tartalmazniuk kell a hibák kijavításának és a javítás jóváhagyásának eljárásait;
2. gondoskodniuk kell a feldolgozások során a feldolgozott vagy visszautasított tranzakciók naplózásáról;
3. biztosítaniuk kell, hogy az adatok teljes körűsége, pontossága és érvényessége a feldolgozási tevékenységek folyamán megmaradjon;

## Adatcsere, adattovábbítás

Az adatcsere, adattovábbítás biztonságáról a szervezetek között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.

A külső szervezetekkel történő adatcserét csak a szervezettel kötött megállapodás alapján lehet végezni, melyben rögzíteni kell az adattovábbítás technikai és adminisztratív eljárásait. Az alkalmazott védelmet az informatikai célrendszer által kezelt és átadott információ biztonsági besorolásának megfelelően kell kialakítani, és a védelmi intézkedéseket a célrendszer biztonsági tervében kell rögzíteni.

A Társasága hálózaton történő elektronikus levelezésre a Microsoft Outlook alkalmazást használja. Az Outlook alkalmazásban a felhasználók csak saját elektronikus levelesládájukhoz férhetnek hozzá.

Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak.

## Hálózati határvédelem

Az elektronikus információs rendszerek csak a Társaságbiztonsági architektúrájával összhangban elhelyezett informatikai biztonsági eszközökön felügyelt interfészeken keresztül kapcsolódhatnak külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

A bizalmas és a nem bizalmas hálózatokat csak a Társaságtűzfalán keresztül lehet összekapcsolni.

A Társaságszámítógép-hálózata egytartományos rendszer. Tilos olyan munkaállomást vagy mobil eszközt csatlakoztatni a Társasághálózatra, amely nem bizalmas hálózati kapcsolattal is rendelkezik, vagy nem tagja a Társaságtartománynak.

A biztonsági adminisztrátorok naprakész nyilvántartást vezetnek az engedélyezett protokollokról, és a hálózati határvédelem informatikai biztonsági architektúra elemeinek beállításairól.

A Társaságszámítógép-hálózatának vezeték nélküli hálózati szegmensein, valamint a nem bizalmas csatornán keresztüli bizalmas kapcsolat során titkosított adatkapcsolatot kell kialakítani.

A titkosított adatkapcsolat technikai specifikációját az ügyvezető hagyja jóvá.

## Hálózati adatátvitel biztonsága

A belső hálózatokon az adatforgalomban kizárólag engedélyezett protokollok használhatók.

A belső hálózaton engedélyezett protokollok körét – az üzemeltetők javaslata, továbbá a biztonsági adminisztrátorok véleménye alapján – az ügyvezető határozza meg.

A belső hálózatokon engedélyezett protokollokról a biztonsági adminisztrátorok naprakész nyilvántartást vezetnek.

Az engedélyezett protokollok körének kialakításakor külön kell kezelni a felhasználók és az üzemeltetők, biztonsági üzemeltetők számára, illetve az átviteli közeg szinten és az állomás szinten engedélyezett protokollokat.

Hordozható számítógépeket, tableteket, okostelefonokat csak a rendszer-üzemeltető által elvégzett ellenőrzés után lehet a Társaságszámítógép-hálózatára kapcsolni.

A Társaságszámítógép-hálózatában a felhasználói hitelesítés adatait (felhasználó azonosító, jelszó) titkosítva kell továbbítani.

## Felelősség

Az adatcsere, adattovábbítás biztonsági eljárásaival kapcsolatos feladatok az ügyvezető (vagy ha van, úgy az általa kijelölt felelős vezető(t)) felelőssége.

# Adatvédelmi hatásvizsgálati eljárásrend

**Cél:** Biztosítani, hogy a Társaságelektronikus információs rendszereiben történő fejlesztéseknél a tervezett adatkezelési műveletek a személyes adatokat megfelelően védjék.

## Alapkövetelmények

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor a Társaságaz adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

1. természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
2. a személyes adatok különleges kategóriáira vonatkozó személyes adatok nagy számban történő kezelése; vagy
3. nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat kiterjed legalább:

1. a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben a Társaságáltal érvényesíteni kívánt jogos érdeket;
2. az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
3. az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
4. a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

A Társaságszükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

## Felelősség

Az adatvédelmi hatásvizsgálat elvégzése az ügyvezető (vagy ha van, úgy az általa kijelölt felelős vezető(t)) felelőssége.

# Jogosultságkezelés

**Cél**: Az erőforrásokhoz és információkhoz való hozzáférési jogok megadásának és megvonásának szabályozása.

## Az információ-hozzáférés szabályozása

Alapelv, hogy minden felhasználó csak azokhoz az erőforrásokhoz és információkhoz férhessen hozzá, amelyek a munkájához mindenképp szükségesek.

A Társaságtulajdonában vagy használatában lévő valamennyi számítógépen tárolt adathoz hozzáférés csak a személyazonosság és a megfelelő jogosultság ellenőrzését követően lehetséges; megvédve az elektronikus információs rendszereket a jogosulatlan hozzáféréstől.

Hitelesítés és azonosítás nélkül csak a Társasághonlapjának publikus oldalai használhatók egyéb felhasználói tevékenység nem.

A különböző alkalmazásokban funkciónként, illetve egyes adatkörökre vonatkozóan szükséges a hozzáférés szabályozása, a jogosulatlanok kizárása. A funkció, illetve adatkörre vonatkozó korlátozások lehetőségét az alkalmazás fejlesztésének időszakában kell megtervezni és az alkalmazást ennek megfelelően implementálni.

A Társaságellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

## A hozzáférési jogok kezelése

A Társaságnem használ külön fizikai hitelesítési eszközöket az információs rendszereihez való hozzáféréshez, csak a felhasználói név+jelszó párost.

Valamennyi információs rendszerhez és szolgáltatáshoz való hozzáférés megadására és visszavonására a Társaságfelhasználó regisztrálási-igénylési, módosítási és regisztráció megszüntetési-visszavonási eljárást kell alkalmazni.

### Igénylés

A Társaságrendszerét használók számára az informatikai biztonsági adminisztrátor hozza létre és vonja vissza a felhasználói azonosítót. Az informatikai biztonsági adminisztrátor nyilvántartást vezet a Társaságelektronikus információs rendszerének felhasználói azonosítóiról, a felhasználók aktuális jogosultságairól. Ezt a nyilvántartást csak az informatikai biztonsági adminisztrátor módosíthatja.

A Társaságba belépő, illetve felhasználói munkakörbe átlépő dolgozóknak a közvetlen vezetője jogosultságigénylő lapot állít ki, amelyben igazolja, hogy a dolgozó jogosult felhasználói azonosító igénylésre.

A jogosultságigénylő lapon a felhasználó közvetlen vezetője illetve a hozzáférésre kijelölt rendszerek adatgazdája meghatározza a dolgozó munkakörét és megjelöli

1. a felhasználó számára munkakörének ellátásához szükséges elektronikus információs rendszereket és jogosultsági csoportokat, továbbá
2. az adott felhasználó esetében a munkakörhöz általánosan meghatározott jogosultsági csoportoktól eltérő további jogosultsági igényeket és az eltérés indoklását. Ez utóbbi esetben is csak a dokumentált jogosultsági csoportot vagy csoportokat lehet megjelölni.

Az egyedi jogosultsági igény nem lehet ellentétes a Társaságfeladatkör-elhatárolási szabályaival.

### Kiadás és érvényesítés

Az informatikai biztonsági adminisztrátor a jogosultságigénylő lap alapján a felhasználóhoz

1. hozzárendel egy felhasználói azonosítót,
2. megadja a felhasználó kezdeti jelszavát, aminek
   * 1. meg kell felelnie a jelszavakkal kapcsolatos szabályoknak és
     2. egyedinek kell lennie, nem használható rendszeresen ugyanaz a karaktersorozat,
3. megadja a felhasználó számára igényelt jogosultságokat
4. a felhasználói azonosítót aktív állapotba helyezi.

Az informatikai biztonsági adminisztrátor a jogosultságigénylő lapon

1. rögzíti a felhasználói azonosítót
2. dokumentálja az azonosító létrehozásának és jogosultságok beállításának időpontját.

Az informatikai biztonsági adminisztrátor nem adhatja meg a jogosultságot, amennyiben megítélése szerint az igényelt jogosultságok nyilvánvalóan megsértik a Társaságfeladatkör-elhatárolási szabályait. Ez esetben az informatikai biztonsági adminisztrátor – a jogosultságigénylő lap másolatának továbbításával és az eljárás felfüggesztésének közlésével – tájékoztatja a szervezet vezetőjét, aki dönt a kérdéses helyzetről.

### Módosítás

A felhasználói azonosító módosítását a felhasználó közvetlen vezetője kezdeményezheti névváltoztatáskor (pl. házasságkötés miatt), valamint a biztonsági üzemeltető az egyes rendszerek felhasználó azonosító konvencióinak szabványosítása miatt és/vagy új azonosító-képző szabályok bevezetésekor.

A felhasználói azonosító módosításakor a kiadás és érvényesítés szabályait kell értelemszerűen alkalmazni.

A felhasználói jogosultságok módosítását kezdeményezheti a felhasználó követlen felettese a munkatárs munkakörének, feladatának megváltozásakor, továbbá a Humánpolitikai csoport.

A jogosultságok módosításakor a kiadás és érvényesítés szabályait kell értelemszerűen alkalmazni.

A felhasználó számára lehetővé kell tenni, hogy jelszavát bármikor, önállóan megváltoztathassa.

Elfelejtett jelszó esetén a felhasználó írásbeli kérésére új jelszót kell kiadni. Ez esetben is a kiadás és érvényesítés szabályait kell értelemszerűen alkalmazni.

### Visszavonás

A felhasználói azonosítókat inaktív állapotba kell helyezni, ha tulajdonosuk munkavégzésre irányuló jogviszonya megszűnt, vagy öt egymást követő sikertelen bejelentkezési kísérlet történt (ilyen esetekben az adott azonosító véglegesen is letiltható).

A Társaságból kilépő vagy más munkakörbe áthelyezésre kerülő dolgozók esetén a felhasználó közvetlen vezetője jogosultságigénylési lapon tájékoztatja az informatikai biztonsági adminisztrátort a jogosultság, illetve a felhasználói azonosító visszavonásáról. (áthelyezés esetén a kiadás és érvényesítés szabályait kell alkalmazni)

Amennyiben a munkaviszony megszüntetés/áthelyezés körülményei alapján feltételezhető, hogy a felhasználó esetleg visszaélésre tesz kísérletet, úgy a közvetlen vezetőnek gondoskodnia kell arról, hogy a jogosultságok (illetve szükség esetén a felhasználói azonosító) visszavonása megtörténjen, mielőtt a dolgozó annak okáról tudomást szerezne.

Az informatikai biztonsági adminisztrátor a jogosultságigénylési lap alapján haladéktalanul törli a felhasználó azonosítóit, visszavonja az összes jogosultságát.

A visszavonási eljárás dokumentálására a kiadás és érvényesítés dokumentációs szabályait kell értelemszerűen alkalmazni.

A Társaságból kilépő dolgozó elektronikus postafiókját, személyes könyvtárának, továbbá az általa használt számítógép(ek) merevlemezének tartalmát (szükség esetén kilépés előtt) archiválni, majd ha az archiválás ellenőrzötten sikeres volt, törölni kell.

### Ellenőrzés

A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amelyek munkájához aktuálisan szükségesek.

A különböző rendszerek biztonsági üzemeltetési kézikönyvének tartalmaznia kell a felhasználói azonosítók, jelszavak és jogosultság

1. kiadásának, módosításának, felfüggesztésének, törlésének
2. megsértés detektálásának (észlelésének), és
3. ellenőrzésének

rendszerspecifikus eljárásait.

Alkalmazás funkciónként, illetve egyes adatkörökre (adatminősítés, biztonsági szint stb. szerint) vonatkozóan szükséges a hozzáférés szabályozása, a jogosulatlanok kizárása.

## Speciális jogosultságok kezelése

Az általános összeférhetetlenségi szabályoktól való speciális eltérés kockázati tényező, ezért az ilyen jogosultságok kiadását mindenképp kerülni kell. Amennyiben valamilyen elkerülhetetlen ok miatt mégis létre kell hozni ilyet, akkor azt csak dokumentáltan, s csak a feltétlenül szükséges időtartamra szabad adni.

A rendszer-segédprogramok használata különös lehetőségeket teremt nehezen ellenőrizhető manipulációkra, ezért ezek használatát különös figyelemmel kell szabályozni és a szabályzatban foglaltakat ellenőrizni. A fejlesztő eszközökhöz, az adatbázisokhoz közvetlen hozzáféréseket lehetővé tevő segédprogramokhoz való hozzáférés csak indokolt esetben engedélyezhető és a tevékenység végén az engedélyt vissza kell vonni, és lehetőleg ki kell zárni az ellenőrizhetetlen származású programok használatát.

Az eljárásrend alkalmazásának hatására csökken annak a kockázata, hogy a speciális jogosultságok nem megfelelő menedzselése miatt a rendszer működésében hibák keletkeznek, vagy illetéktelen helyre kerülnek védendő adatok.

## A felhasználói jelszókezelés

A jelszavak felhasználói kezelését szabályozni kell, figyelve arra, hogy a felhasználók titokban tartsák, és megfelelő időközönként változtassák jelszavaikat. Emellett biztosítani kell, hogy a jelszavak kiosztásakor, illetve használatakor csakis a tulajdonos szerezzen tudomást a jelszóról.

Annak érdekében, hogy a jelszavakkal történő hitelesítés kellően megbízható legyen, gondoskodni kell arról, hogy:

1. a jelszavak legalább nyolc karakterből álljanak,
2. lehetőleg vegyesen kis és nagybetűket, számokat és írásjeleket is tartalmazzanak,
3. a kezdeti jelszót az első belépés alkalmával kötelezően meg kelljen változtatni,
4. a jelszavakat minden hat hónapban ki kell cseréltetni a felhasználóval.

A jelszavakat tartalmazó fájlokat (illetve ezeknek a jelszavakat tartalmazó részét) visszafejthetetlen (egyirányú) kódolással kell tárolni, ezekhez az állományokhoz hozzáférési jogosultságot csak az informatikai biztonsági adminisztrátorok kaphatnak.

A jelszavakat tartalmazó fájlok sérülését, jogosulatlan hozzáférési kísérleteket az informatikai biztonsági adminisztrátornak azonnal jelentenie kell az Informatikai csoportnak.

A jelszavak titkosak, ezért azokat minden felhasználó köteles úgy kezelni, hogy rajta kívül más tudomására ne jusson.

Tilos a jelszót:

1. más tudomására hozni,
2. más számára ismert vagy hozzáférhető, vagy látható helyen (pl. monitororra ragasztva) tárolni,
3. úgy megválasztani, hogy az adott személyre jellemző és ezért könnyen kitalálható legyen.

Az elektronikus információs rendszerekbe való bejelentkezés során, továbbá a jelszó megváltoztatásakor gondoskodni kell arról, hogy

1. a jelszavak azonosíthatatlanul jelenjenek meg a képernyőn és
2. titkosítva legyenek a hálózati adatátvitel során.

Az egyes rendszerekre vonatkozóan az egyes különleges jogosultságokat biztosító felhasználói azonosítókat (pl: adminisztrátor, root, stb. a továbbiakban: speciális felhasználók) az üzemeltetők és informatikai biztonsági adminisztrátorok adatszolgáltatása alapján az Informatikai csoport tartja nyilván.

A speciális felhasználókhoz tartozó jelszavakra a következő különös szabályok vonatkoznak:

1. a speciális felhasználók jelszavait lezárt borítékban az Informatikai biztonsági vezető páncélszekrényében kell őrizni;
2. speciális felhasználók jelszavához csak indokolt esetben lehet hozzáférni;
3. a boríték felbontásáról minden esetben jegyzőkönyvet kell készíteni, megjelölve a speciális felhasználó igénybe vételének pontos okát és a felbontók személyét;
4. gondoskodni kell arról, hogy a szükséges műveletek elvégzése után a speciális felhasználó számára új jelszó kerüljön kiadásra és azt haladéktalanul, lezárt borítékban ismét az Informatikai biztonsági vezető páncélszekrényébe kell helyezni.

### Felhasználói felelősségek

A felhasználók a Társaságelektronikus információs rendszereihez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezettek, ahol nyilatkozatukkal igazolják, hogy az elektronikus információs rendszer használatához kapcsolódó, rájuk vonatkozó biztonsági szabályokat és kötelezettségeket megismerték, saját felelősségükre betartják.

A jelszavakkal kapcsolatos szabályok megszegéséből, így különösen a más jelszavának megismerésével elkövetett esetleges visszaélés következményeiért a szabályokat megszegő felhasználók a felelősek.

A Társaságévente legalább egy alkalommal felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet a viselkedési szabályok betartását. Változás esetén a hozzáférési nyilatkozatot az érintett felhasználókkal ismételten aláíratja.

## Felhasználói informatikai biztonsági követelmények

A hálózati bejelentkezéshez a felhasználóknak felhasználónévvel és jelszóval kell azonosítaniuk magukat.

A munkaállomásokon telepített operációs rendszert úgy kell beállítani, hogy ha a munkatárs 5 percen túl nem használja a rendszert, az automatikusan lezárja a munkaállomást, és a munka újbóli megkezdésekor felhasználónév, jelszóval kell a munkatársnak azonosítania magát.

A külső felhasználókat a kapcsolati alrendszerek megfelelő kialakításával, a belső felhasználókat (alkalmazottakat) szabályzatokkal kell kötelezni arra, ha őrizetlenül hagyják a berendezéseiket, akkor (akár logikailag, akár fizikailag) zárják le azokat.

A belső felhasználókat (alkalmazottakat) kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.

## Nyilvánosan hozzáférhető információk kezelése

A Társasága nyilvánosan hozzáférhető információkat a honlapján teszi közzé.

A nyilvánosan hozzáférhető információk (beleértve a közérdekű adatokat) sértetlensége érdekében adminisztratív és technikai intézkedéseket kell kidolgozni, melyben ki kell térni az információ változtatásának eljárásrendjére, új információ közzététele előtt követendő eljárásra és egyes információk törlésének eljárásaira is.

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.

## Távmunka és távoli elérés szabályai

Szabályozni kell, hogy a biztonságos távoli hozzáférés, illetve munkavégzés érdekében milyen tevékenységek és technikai feltételek szükségesek. Távoli hozzáférés és munkavégzés csak indokolt esetben engedélyezhető, és a hozzáférés, adatcsere biztonsága érdekében külön eljárásokat kell meghatározni és megvalósítani.

A mobil számítógépek (notebook, okostelefon, tablet, pda, stb.) biztonságos használatának érdekében szabályozni kell ezen eszközök esetében a hozzáférést, a logikai és fizikai biztonságot, az adatmentések megvalósítását, illetve a biztonságos környezeten kívüli munkavégzés szabályrendszerét.

A külső összeköttetéseket csak a feltétlenül munkaidőn kívül is elérni szükséges rendszerekhez szabad engedélyezni.

Külső rendszerből a Társaságbelső hálózatára csak a Társaságelőzetes írásos engedélyével csatlakozhat bárki. A megvalósulás műszaki feltételeit az informatikai biztonsági vezető határozza meg (pl. VPN).

A felhasználókkal a szolgáltatások indítása, vagy az azokkal történő kommunikáció megkezdése előtt végre kell hajtani a hitelesítési eljárást.

Az adott hálózati alrendszer hitelesítési mechanizmusa nem érintheti a hálózat többi alrendszerének hitelesítési rendszerét.

A hálózati erőforrások használatát a felhasználók számára korlátozni kell.

Megosztott erőforrások csak azonosítás és hitelesítés után legyenek elérhetők. Munkaállomások megosztását (azok védelmének nehézsége miatt) kerülni kell.

Biztosítani kell a fogadó oldalon a felhasználó azonosítás utáni visszahívásának (call back) lehetőségét.

Csak a kellően biztonságos környezettel, technikákkal biztosított helyeken lehet a távoli elérést biztosítani.

Távoli elérésre külön kezelt felhasználói csoportot kell kialakítani

Külső rendszerből csak olyan csatlakozás engedélyezhető, amely során a felhasználó csak adatellenőrzésre, és –feldolgozásra képes. Adatmásolás, tárolás vagy továbbítás távoli rendszerbe nem engedélyezhető ilyen kapcsolat esetében.

Szabályozni kell, hogy mekkora az inaktív vagy teljes időtartam, amely után az adatkapcsolatot meg kell szüntetni. Ezt az időintervallumot figyelembe kell venni a rendszerek paraméterezésénél, illetve az alkalmazások fejlesztésénél. Az időtartam betartandó attól függetlenül, hogy humán beavatkozásról vagy alkalmazás automatikus aktivitásról van szó.

## Felelősség

A hozzáférés-ellenőrzés szabályainak elkészítése, felülvizsgálata, használatának ellenőrzése az ügyvezető (vagy ha van, úgy az általa kijelölt felelős informatikai biztonsági vezető) hatáskörébe tartozik.

# Adatmentés

**Cél:** Az elviselhetetlen mértékű adatvesztés megakadályozása, és az elvárt időn belüli adatvisszaállítás biztosítása.

## Információk biztonsági mentése

Minden, a Társaságkezelésében vagy használatában lévő, elektronikus formában tárolt információról biztonsági mentéseket kell készíteni.

Olyan mentési rendet kell kialakítani, ami biztosítja az adatok visszaállíthatóságát a Társaságáltal meghatározott követelmények szerint (elvárt visszaállítás idő, maximálisan elviselhető adatvesztés stb.).

A mentések gyakoriságát, a mentés módját, a használt adathordozót és a tárolási helyet a fentiek figyelembevételével kell kiválasztani, és ki kell dolgozni azokat az eljárásokat, amelyek teljesítik a követelményeket.

Az eljárások kidolgozása után az érintettek számára oktatás szükséges, és elengedhetetlen a teljes visszaállítási eljárás tesztelése is.

Ki kell dolgozni a mentések ellenőrzésének (ellenőrző visszatöltés) rendjét is (többpéldányos mentés, külső helyszínen tárolás).

A mentési, visszaállítási eljárást évente és releváns változások esetén felül kell vizsgálni, és naprakésszé kell tenni.

## Mentési eljárás

Biztonsági mentéseknek kell készülnie

1. az online elérhető (éles, tartalék, teszt) adatbázisokról és fájlrendszer könyvtárakról,
2. az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról,
3. szoftverek telepítőkészletéről.

Normál (Teljes-FULL): azaz minden mentési folyamattal mentésre kerül az összes állomány, függetlenül az előző mentés időpontjától és annak státuszától.

Inkrementális: azaz csak az előző mentés óta változott állományok kerülnek mentésre.

Az alábbi táblázat összefoglalóan tartalmazza az adatmentések gyakoriságát és az alkalmazott mentési típust:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Forrás | H | K | Sz | Cs | P |
| Levelezőszerver | INC | INC | INC | INC | FULL |
| Fileserver | INC | INC | INC | INC | FULL |
| INTERNETSERVER | INC | INC | INC | INC | FULL |

A mentéseket ütemezett feladatként, automatikusan kell elvégezni, minden hétköznap.

Az automatikus mentés elindítását munkaidőn túl kell ütemezni, hogy az alkalmazások ne legyenek használatban és ne legyenek nyitott állományok. Emiatt az automatikus mentést 22:00-ra kell ütemezni. A mentés eredményességét és futási idejét a mentés másnapján az informatikai biztonsági adminisztrátornak kell ellenőriznie. Minden rendellenességet jeleznie kell az informatikai biztonsági vezetőnek.

A mentés a Backup számítógépre való másolással történik.

Az adatbázis szerverek saját mentést készítenek, melyeket szintén a Backup számítógépre kell másolni.

## Archiválási eljárás

Az előző heti napi mentések közül a pénteki mentést kell archiválni hétfő reggel. Az archiválás során a pénteki mentést kifejezetten erre a célra beszerzett külső merevlemezre (HDD-re) kell átmásolni.

Az archivált állományokat tartalmazó HDD-ket egyedi azonosítóval kell ellátni, és tűzálló páncélszekrényben kell tárolni. A HDD-kről nyilvántartást kell vezetni.

Az archiválást az Informatikai biztonsági vezető, vagy az általa kijelölt informatikai munkatárs jogosult elvégezni.

Az archiválás után az utolsó hét előtti napi mentéseket törölni kell.

Az archivált állományokat tartalmazó HDD-ket évente selejtezni kell. A selejtezés során az egy éven túli archív állományokat tartalmazó HDD-ket alacsony szintű formázással formattálni kell. Az archív állományok selejtezéséről jegyzőkönyvet kell rögzíteni.

## Visszatöltés mentési állományból

A visszatöltés igénylését az adott szervezeti egység vezetője írásban kezdeményezheti az Informatikai biztonsági vezetőnek címzett e-mail-ben. Az e-mail-nek tartalmaznia kell, hogy

1. melyik állomány visszatöltését igényli;
2. milyen dátumú állomány visszaállítását igényli;
3. milyen célból igényli az állomány visszaállítását

Az Informatikai biztonsági vezető megvizsgálja, hogy milyen okai vannak a visszatöltési igénynek. Ezek lehetnek:

1. adatvesztés/programhiba;
2. felhasználói hiba;
3. természeti katasztrófa.

Amennyiben adatvesztés vagy programhiba történt, az Informatikai biztonsági vezető gondoskodik a hiba elhárításáról. Katasztrófa esetén a Katasztrófatervnek megfelelően jár el.

Az Informatikai biztonsági vezetőnek meg kell vizsgálnia, hogy a visszatöltéssel nem sérülnek, illetve változnak meg az adott rendszer adatai. A visszatöltés jogosságát az Informatikai biztonsági vezető dönti el az adott rendszer adatgazdájával történt egyeztetés után. Amennyiben az ellenőrzés nem talált kizáró okot, és a visszatöltési kérelemben megadott dátumú mentés elérhető, az adott napi állományt vissza kell tölteni a kért helyre.

A sikeres visszatöltés tényét jegyzőkönyvben kell rögzíteni

## Felelősség

Az adatmentések felelőssége az ügyvezető (vagy ha van, úgy az általa kijelölt felelős informatikai biztonsági vezető) hatáskörébe tartozik.

# Biztonsági helyzet- és eseményértékelés

**Cél:** Gondoskodni arról, hogy a biztonsági események és zavarok okozta kár minimális legyen, továbbá hogy a véletlen biztonsági eseményeket megfigyelés alatt tartsák és azokból okuljanak.

## Naplózás

A Társaságelektronikus információs rendszereiben automatikus naplót kell vezetni az elektronikus információs rendszerek biztonsági szempontból lényeges tevékenységeiről.

A különböző naplóbejegyzésekben be kell gyűjteni elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

Az informatikai biztonsági adminisztrátor egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást.

Az informatikai biztonsági vezető megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

Az automatikusan készülő naplókban (naplóbejegyzés generálás) rögzíteni kell legalább az alábbi eseményeket:

* be- és kijelentkezéseket;
* sikertelen bejelentkezési kísérleteket;
* jogosulatlan hozzáférési kísérleteket;
* jogosultság megadáskor a megadott jogosultságokat;
* az operátori konzol riasztásait és üzeneteit;
* a rendszerriasztásokat, meghibásodási jelentéseket;
* felhasználók felvételét, törlését;
* jogosultsági csoportokban beálló változásokat (új csoport létrehozása, jogosultsági csoporthoz tartozó elemi jogosultságok megváltozása, stb.);
* felhasználók jogosultságaiban beálló változásokat;
* naplózási funkciók indítását és leállítását
* naplóállomány létrehozását, törlését; (külön jegyzőkönyvben rögzítve);
* a naplózási konfigurációban beálló változást (külön jegyzőkönyvben rögzítve);
* a rendszerdátum, -idő megváltoztatását;
* hardverkonfiguráció megváltozását;
* nyilvános hálózaton keresztüli kapcsolat
  + létrehozása és bontása
  + ellenoldali fél azonosítása
  + forgalom jellege
  + továbbított vagy fogadott állomány neve, elérési útvonala.

Az eseményekhez a naplózó funkciónak hozzá kell rendelnie (amennyiben értelmezhető):

* a felhasználó azonosítóját,
* a számítógép azonosítóját (IP cím),
* a dátumát és időpontját, (a rendszernek a belső rendszerórát kell használnia a naplóbejegyzések időbélyegeinek előállításához, és időbélyegeket kell rögzítenie)
* a hozzáféréskor elért állományokat,
* a használt programot.

A különböző rendszerek naplóállományainak egységes értelmezhetőségének érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:

* ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen,
* a naplózást a lehető legkevesebb számú naplóállomány használatával történjen,
* automatikus mechanizmus gondoskodjon az egyes eszközök rendszerórájának szinkronizálásáról,
* automatizált megoldások támogassák a különböző naplóállományok összefésülését, feldolgozását és elemzését.

A naplóállományokhoz írási jogosultsággal humán felhasználók nem férhetnek hozzá, a naplóállományokból a törlés nem engedélyezett.

Biztosítani kell, hogy az elektronikus információs rendszer megvédje a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

A naplóbejegyzéseket a Társaságinformációmegőrzési követelményeknek megfelelő időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

Az informatikai biztonsági vezető lehetővé teszi az adatgazdák és a Társaságszámára, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire.

## Incidenskezelés

Az informatikusoknak naponta ellenőriznie kell a naplóállományok bejegyzéseit.

A Társaságfolyamatosan figyeli a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseit (<http://www.cert-hungary.hu/aggregator/sources/2> ), és az egyéb forrásból érkező riasztásokat.

Incidens esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén a Társaságinformációrendszerének automatikusan jelentést kell generálnia és elküldenie az informatikusoknak és az üzemeltetés vezetőjének.

Az információbiztonsági szabályok megsértéséről az informatikusoknak jelentést kell tennie az informatikai biztonsági vezetőnek, aki:

* minősíti az incidenst a körülmények ismeretében, vagy
* eseti szakértői csoportot hoz létre az incidens körülményeinek kivizsgálására.

Az informatikai biztonsági vezető, az incidens súlyának ismeretében dönt a következményekről, az incidens kezeléséről a hibák javításáról.

A biztonsági esemény kivizsgálásának eredményéről az üzemeltetés vezetője értesíti a szervezet vezetőjét, aki dönt a további esetleges fegyelmi, jogi eljárásról.

Az informatikai biztonságban résztvevők és szükség szerint az informatikai vagy szakmai rendszergazdák bevonásával a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárniuk:

* figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó részeket.
* amennyiben a Társaságrendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni.
* amennyiben a Társaságnem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni.
* amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külsős szakértőket kell bevonni az elhárítás folyamatába.

Amennyiben a sérülékenység jellege olyan, hogy annak elterjedése megelőzhető, hogyha a felhasználók például nem nyitnak meg bizonyos weboldalakat vagy egy adott jellegű elektronikus levélben található linkre nem kattintanak, akkor belső figyelmeztetést kell kiadni a Társaságszokásos értesítési rendszerén (pl. e-mail) keresztül.

### Bejelentési kötelezettség

A Társaságnál amennyiben felmerül a gyanú, hogy számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van, akkor a jogszabályokban meghatározott esemény bejelentési kötelezettség mellett bejelenti ezen incidens tényét és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel is.

Amint a Társaságtudomására jut egy esetleges az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásukra jutott, bejelenteni kötelesek az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudják, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az adatvédelmi incidensről szóló bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) mindenkori kapcsolati pontjára (<http://naih.hu/uegyfelszolgalat,--kapcsolat.html>) kell eljuttatni.

A bejelentés összeállításának és beadásának felelőse az adatvédelmi tisztviselő, ha a Társaságban van ilyen kijelölt felelős, vagy az informatikai biztonsági vezető.

Az adatvédelmi incidensről szóló bejelentésben legalább:

1. ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
2. közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
3. ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
4. ismertetni kell a Társaságáltal az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

A Társaságnyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

### Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaságindokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az előző pont b), c) és d) pontjában említett információkat és intézkedéseket.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

1. a Társaságmegfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
2. a Társaságaz adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
3. a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

## Ügy és üzemmenet-folytonosság

A Társaságnak azonosítania kell a kritikus működési folyamatokat és beépítenie a működésfolytonosságot az informatikai biztonság irányítási követelményeibe más folytonossági követelményekkel, amelyek olyan szempontokra vonatkoznak, mint műveletek, személyzettel való ellátás, anyagok, szállítás és eszközök.

Az üzemzavarok, biztonsági meghibásodások, szolgáltatás-elvesztés és szolgáltatás rendelkezésre-állási követelményeit működési hatáselemzésnek kell alávetni.

Az ügy és üzemmenet-folytonosság részletes szabályait, valamint a biztonsági események bekövetkeztekor követendő eljárást, ideértve az adatok sérülését és a helyreállítást is, a Társaságügymenet-folytonossági és katasztrófaelhárítási (BCP/DRP) terve [3] szabályozza.

## Felelősség

A biztonsági helyzet- és eseményértékelés az ügyvezető (vagy ha van, úgy az általa kijelölt felelős vezető(t)) hatáskörébe tartozik.

# Adatkezelési kérés- és panaszkezelés

**Cél:** Gondoskodni arról, hogy a Társaságáltal kezelt személyes adatokról az érintett adatalanyok a megfelelő hatékonysággal és minőségben kapjanak információt és segítséget.

## Alapelvek

A Társasága különböző oktatásain és tréningjein kiemelt figyelmet fordít arra, hogy az érintett magánszemélyek részére a személyes adatok kezelésére vonatkozó, az alábbiakban ismertetettvalamennyi információt és tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Az oktatások, tréningek és tájékoztatók különösen fontosak az ügyfélkapcsolati pontokon, mint például:

* titkárság (telefon, e-mail),
* központi e-mail,
* ügyfélszolgálat, stb.

A fenti helyeken dolgozó kollégáknak mindig pontosan tisztában kell lenniük az adatkezelési elvekről és jogszabályokról, a vonatkozó felelősségi körökről, a megfelelő kommunikációról és válaszadási normákról.

A Társaságindokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, a Társasága személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

1. a Társaságképviselőjének a kiléte és elérhetőségei;
2. az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
3. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
4. a Társaságvagy harmadik fél jogos érdekei, ha van ilyen;
5. adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
6. adott esetben annak ténye, hogy a Társaságharmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

## Az érintett jogai

Az érintett jogosult arra, hogy a Társaságtól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

1. az adatkezelés céljai;
2. az érintett személyes adatok kategóriái;
3. azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
4. adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
5. az érintett azon joga, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
6. a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
7. ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
8. az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a megfelelő garanciákról.

A Társaság az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért a Társaság az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, a Társaság pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

1. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
2. az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
3. az érintett az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
4. a személyes adatokat jogellenesen kezelték;
5. a személyes adatokat a Társaságra alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
6. a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Az érintett jogosult arra, hogy kérésére a Társaság korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

1. az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát;
2. az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
3. a Társaságnak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
4. az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A Társaság minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

Az érintett jogosult arra, hogy a rá vonatkozó, általa a Társaság rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa, ha:

1. az adatkezelés hozzájáruláson, vagy szerződésen alapul; és
2. az adatkezelés automatizált módon történik.

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen, ideértve az ezeken alapuló profilalkotást is, ha:

1. az adatkezelés közérdekű vagy a Társaságra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
2. az adatkezelés a Társaság vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Ebben az esetben a Társaság a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

## Az érintettek kéréseinek kezelése

Az érintettek kérései bármilyen kommunikációs csatornán befuthatnak a szervezetbe, de a legvalószínűbbek:

* személyesen az ügyfélszolgálaton,
* telefonon az ügyfélszolgálaton vagy máshol,
* elektronikus levélben,
* hagyományos levélben, vagy faxon.

Az érintettek kérései lehetnek például:

* adatkérés (milyen adatokat kezel róla a szervezet),
* adatmódosítási kérés,
* adathasználat korlátozás,
* adatletiltás,
* az adatok „elfelejtésének” kérése.

Minden beérkezési csatorna, és bármilyen kérés esetén az érintettek kérését pontosan, változtatás nélkül és haladéktalanul továbbítani kell az informatikai biztonsági vezetőnek.

Az érintettekkel kapcsolatos:

* minden kérés kezelése,
* a szükséges adatok begyűjtése,
* az esetleg szükséges szervezeti vagy technikai módosítások elvégzése,
* a kérések megválaszolása

az informatikai biztonsági vezető felelőssége.

Az informatikai biztonsági vezető köteles az adatkérő személyazonosságát (jogosultságát) ellenőrizni, a kért adatok megadásáról, vagy a szükséges feladatok elvégzéséről intézkedni, és a rendelet által megszabott határidőn belül a megfelelő választ az érintettnek megküldeni.

## Felelősség

A kérés- és panaszkezelés koordinálása és végrehajtása az ügyvezető, vagy az általa kijelölt felelős hatáskörébe tartozik. Az ellenőrzési felelősség a szervezet vezetőjére hárul.

# Oktatás, képzés, tudatosítás

**Cél**: Folyamatosan gondoskodni arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek, és motiválva legyenek a szervezet információvédelmi szabályzatainak és intézkedéseinek a betartására. A felhasználók legyenek oktatva a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében.

## Számítógéphasználati elvek

A Társaság minden dolgozója jogosult a munkaköréhez tartozó adat- és információ hozzáféréshez, azok felvitelére és karbantartásra.

A Társaság minden belépő új munkatársa köteles a belépésével egyidejűleg az Informatikai biztonsági szabályzatban és kapcsolódó dokumentumaiban foglaltakat elolvasva megismerni, tudomásul venni.

A Társaság az információ feldolgozó eszközöket (számítógépeket, nyomtatókat, fénymásoló- és fax berendezéseket, scannereket, stb.) munkavégzés céljára biztosítja az azokat felhasználó munkavállalóknak.

Az Informatikai biztonsági szabályzatban és kapcsolódó dokumentumaiban foglaltak be nem tartása szankcionálást von maga után, amely akár a munkaviszony megszűntetését, polgári peres vagy büntetőeljárást is magába foglalhat. A Társaság fenntartja magának a jogot, hogy a bármely felhasználó számára dedikált előjogokat, kiváltságokat azonnali hatállyal visszavonja, illetve megszűntesse.

A szervezet vezetője, a közvetlen vezetők, az informatikai biztonsági vezető azonnal köteles intézkedést kezdeményezni a Társaság munkatársával vagy a külső munkatárssal szemben, amennyiben azok megsértik az Informatikai biztonsági szabályzatban és kapcsolódó dokumentumaiban foglaltakat.

A felhasználók kötelesek megőrizni a Társasággal kapcsolatos információk bizalmasságát, függetlenül az információhordozó formájától, amely lehet szóbeli, papíralapú illetve elektronikus.

A szervezet vezetője köteles a szükséges intézkedéseket megtenni, amennyiben az adatvédelemre, a számítógép vagy az internet használatra vonatkozó eljárásokat a saját vagy külsős munkatárs megsérti.

A felhasználók semmilyen szoftvert nem telepíthetnek az Informatika munkatársának jóváhagyása nélkül, beleértve az Internetről letölthető vagy máshonnan beszerzett ingyenes vagy időszakosan szabadon felhasználható programokat. Új szoftver telepítésének igényét a közvetlen vezetőnek kell bejelenteni.

A szoftverek jogtisztaságára vonatkozó feladatokat, kötelezettségeket és szankciókat a dolgozók munkaköri szerződésben is rögzíteni szükséges.

## Internet használata

Mivel a Társaság számára az Internet kapcsolat üzletileg kritikus, ezért az Internetet használó munkavállalóknak az alábbi szabályokat kell betartaniuk:

* Tilos az Internet illegális (jogszabályokba ütköző) célokra történő használata, mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; software szándékos és tudatos illegális terjesztése,
* Tilos másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység,
* Tilos az Internet hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik.
* Tilos a nem a Társaság tevékenységéhez kapcsolódó profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
* Tilos a hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység,
* Tilos a hálózatot, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybevevő tevékenység,
* Tilos az Interneten honlappal rendelkező szállítók, szolgáltatók, azok termékeinek, szolgáltatásainak minősítése,
* Tilos a Társasághoz méltatlan oldalak keresése, látogatása,
* A felhasználók nem tölthetnek le, illetve nem tölthetnek fel az Internetre semmilyen olyan jellegű információt, adatot, szoftvert, amely összeférhetetlen a Társaság Informatikai biztonsági politikájával [2].
* Tilos az Internetről letöltött szoftverek (shareware vagy freeware termékek) a Társaság informatikai eszközein történő telepítése.
* A szervezet vezetőjének, a közvetlen vezetőknek, az informatikai biztonsági vezetőnek és az általuk megbízott személyeknek jogában áll a felhasználók előzetes értesítése nélkül is bármely weboldal látogatását megtiltani, illetve a weboldalak látogatását oly módon szabályozni, hogy tételesen megadja a látogatható helyek körét.

## e-mail, elektronikus levelezés

A Társaság levelezőrendszerében minden munkatárs rendelkezik személyes, kizárólag általa kezelhető postafiókkal, amit csak és kizárólag munkavégzésre használhat. A levelezőrendszerhez tartozó megosztott postafiókokhoz történő hozzáférés előre meghatározott jogosultság alapján történik Ennek kezelése során be kell tartani a vonatkozó jogszabályokat, és a Társaság szabályzatait. Az előírások be nem tartása, azok megszegése a mértékétől függően munkajogi, vagy a megvalósított tényállástól függő egyéb szankció alkalmazandó.

A levelező rendszer működését az informatikai csoport monitorozza és működteti.

A Társaság levelezőrendszerében folytatott minden tevékenységet az előző fejezetekben leírt elveknek megfelelően kell folytatni. Ezeknek az elveknek a betartását a Társaság vezetése külön figyelmeztetés nélkül is ellenőrizheti, és erről a tényről a munkaszerződésben, a számítógépes jogosultság kiosztásakor, vagy munkáltatói utasításban tájékoztatja a felhasználóit. E tájékoztatásnak ki kell terjednie arra, hogy az ellenőrzés milyen célból történik (például a látogatott internetes oldalak és a látogatás időtartamának megfigyelése a munkaidő alatti munkavégzés ellenőrzése okán), az adatokat meddig kezelik (a mentéseknek köszönhetően hány évig ellenőrizhető vissza a levelek tartalma), és az adatkezeléssel kapcsolatban milyen jogai vannak az érintett személynek. A fenti tájékoztatást a munkavállalónak írásban is tudomásul kell vennie.

Az elektronikus levelezés esetleges munkáltatói ellenőrzése minden esetben célhoz kötött, aminek a levelek ellenőrzése, megőrzése minden szakaszában meg kell felelni.

A levelezési rendszer paramétereit, beleértve a szűrőfeltételeket, korlátozásokat (mellékletek szűrése: nagyméretű multimédiás file-ok, futtaható file-ok) az informatikai csoport állítja be, az üzleti és biztonsági követelmények figyelembe vételével a Társaság vezetőjének egyidejű tájékoztatása és engedélye alapján.

## Közösségi média használata

A közösségi média eszközein és felületein munkaidőben és/vagy a Társaság informatikai rendszeréből történő kommunikáció nem lehet személyes célú, csak munkával kapcsolatos. A közösségi média használata nem történhet a munkával kapcsolatos kötelezettségek teljesítésének rovására.

A közösségi média felületeken a munkatársaknak tilos bármilyen olyan tartalom közzététele, amely alkalmas lehet a Társaság jó hírnevének, jogos gazdasági érdekének veszélyeztetésére.

A munkatársak számára a közösségi média felületeket tilos mások bárminemű zaklatására, megfenyegetésére, rágalmazására vagy becsmérlésére használni.

Tilos megosztani a közösségi média felületeken a Társaság által "üzleti titoknak" és/vagy "szigorúan bizalmasnak" minősített információkat, ide értve a Társaság belső működésére, folyamataira, infrastruktúrájára vezetőségére, munkavállalóira vonatkozó információkat is.

Tilos a Társaság székhelyén, telephelyein és irodáiban készült fényképek, hang- és videó felvételek megosztása.

**A személyes adatok védelme:** felesleges és személyes érzékeny információt a kollégáink ne osszanak meg senkivel, se e-mail, se közösségi médián keresztül. Nem adhatnak meg, vagy oszthatnak meg személyes adatokat, lakhely-, születési adatokat, telefonszámot, (védett) e-mail címet, bankszámlaszámot, bankkártya adatokat (főleg PIN kódot), semmilyen jelszót. Nem tehetnek közzé önmagukról és a környezetükről kompromittáló fényképeket, videókat, vagy olyanokat, amikből szenzitív információkra lehet szert tenni.

**Megfelelő tartalmak:** a közösségi média eszközein – különösen - munkaidőben történő kommunikáció megfelelő professzionalizmust kell, hogy visszatükröződjön, megfelelő hangnemet használva. Így például a vulgáris kifejések, mást megalázó viccek nem megengedettek.

**Becsületesség:** a közösségi média felületein megjelentetett publikáció, illetve véleménynyilvánítás minden esetben legyen etikus és félreérthetetlen. Érdemes azt is kinyilvánítani, hogy a szóban forgó tartalom magánvélemény, azaz szubjektív, és nem fogalmaz meg semmilyen objektív, pozitív/negatív kritikát.

## Oktatási eljárásrend

A szervezet valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is, megfelelő képzésben kell részesíteni a szervezet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. Az informatikai biztonságtudatossági képzés elvégzését az elektronikus információs rendszer használója aláírásával igazolja. Aláírásként elfogadható a Társaság belső elektronikus információs rendszerén belül érkezett egyértelmű és pontosan beazonosítható elektronikus visszajelzés is (e-mail, intranetes „elfogadom/tudomásul vettem” stb.)

Kiemelten fontos az adatkezelési műveletekben vevő személyzet tudatosság-növelése és képzése. Az ilyen felhasználóknak pontosan tisztában kell lenniük a mindenkori adatkezelési rendelkezésekkel, azok etikai és jogszabályi vonatkozásaival, az ebből fakadó személyes kötelezettségeikkel és felelősségeikkel.

E képzés nélkül a Társaság elektronikus információs rendszereit használni tilos.

A képzést azelőtt kell lefolytatni, még mielőtt a felhasználók megkapnák a hozzáférési jogot (jogosultság) az elektronikus információs rendszerekhez, vagy az adatokhoz.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell a szervezetben, különleges biztonsági képzés is szükséges az informatikai biztonsággal foglalkozó személyzet számára. A biztonsági képzés mélységének az informatikának a szervezeten belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia.

## Felelősség

Az oktatás megszervezése, a tematika kidolgozása és az előadás megtartása az ügyvezető (vagy ha működik olyan, úgy az informatikai biztonsági vezető) hatáskörébe tartozik.

# Ellenőrzési eljárásrend

**Cél**: Folyamatosan gondoskodni arról, hogy a szabályzatban foglaltak a megfelelő módon kerülnek alkalmazásra.

## Általános elvek

Az informatikai biztonsági szabályzatban előírt eljárások és szabályok érvényesítése hagyományos vezetési eszközökkel történik, melynek elemei:

* eseti vagy rendszeresen ismétlődő ellenőrzés (továbbiakban: ellenőrzés);
* felelősségre vonás az ellenőrzéssel feltárt mulasztás miatt (továbbiakban: felelősségre vonás).

Az informatikai biztonság jelen szabályzatban foglaltaknak megfelelő szinten történő fenntartása érdek-ében megfelelő kontrollokat kell kialakítani. A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen.

Ennek érdekében meg kell határozni az ellenőrzések területeit, és minden területhez külön-külön meg kell fogalmazni az ellenőrzési célkitűzéseket.

Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit.

Az ellenőrzés eredményét minden esetben ki kell értékelni, és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Bizonyítható mulasztás feltárása esetén szükség szerinti mértékű felelősségre vonási eljárást kell kezdeményezni.

Az ellenőrzéseket egyes dokumentumok, teljes dokumentációk vizsgálatával, személyes beszámoltatással és helyszíni szemlék alapján lehet végrehajtani.

## Az ellenőrzések területei, célkitűzései

Az informatikai biztonsággal kapcsolatos ellenőrzések az alábbiak:

* **Megfelelőségi vizsgálat**: célja felderíteni, hogy a Társaság rendelkezik-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e.
* **Az informatikai biztonság szintjére vonatkozó vizsgálat:** célja felderíteni, hogy az informatikai biztonság szintje megfelel-e a Társaság üzleti elvárásainak.
* **Az informatikai biztonsági szabályok betartásának ellenőrzése:** Célja felderíteni, hogy a Társaság informatikai biztonsági szabályait az illetékes személyek ismerik-e, illetve betartják-e. Ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető.

## Felelősség

Az ellenőrzések megszervezése és végrehajtása az ügyvezető (vagy, ha van, úgy az ügyvezető által kijelölt felelős) hatáskörébe tartozik.

# Hivatkozások

|  |  |  |
| --- | --- | --- |
| **No** | **Dokumentum azonosító** | **Dokumentum cím** |
| 1. | 2016/679 rendelet | Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) |
| 2. | Informatikai\_biztonsági\_politika.doc | A TÁRSASÁGInformatikai biztonsági politikája |
| 3. | BCP\_DRP\_terv.doc | A TÁRSASÁGügymenet-folytonossági és katasztrófaelhárítási (BCP/DRP) terve |
|  |  |  |

# Dokumentum történet

|  |  |  |  |
| --- | --- | --- | --- |
| **Dátum** | **Verzió** | **Módosította** | **Módosítás oka** |
| 2018. május 25. | 1.0 | ügyvezető | Ez a dokumentum első változata |

© TMSI Kft. 2017. nov: 753951+VP7751