# Információ Biztonsági Szabályzat (IBSZ)

A Szabályzás célja az GDPR rendelet alapján elvárható szabályozási célok és intézkedések, a Kozármislenyi Közös Önkormányzati Hivatal (továbbiakban: Szervezet) történő megvalósulási módjának rögzítése.

A szabályozó dokumentumot jóváhagyom,

**alkalmazását XXX napjától elrendelem**

**…….**

**Dr. Bíró Károly**
**Polgármester**

# A dokumentum módosításainak jegyzéke

A dokumentum kötelező felülvizsgálatát adott év zárásakor el kell végezni, úgy hogy az esetleges módosítások hatálybalépésére következő év január 1-jén sor kerüljön.

| Verzió | Dátum | Leírás | Jóváhagyó |
|---|---|---|---|
| 1. | 2019.03.21 | GDPR megfeleltetés | **Dr. Bíró Károly** |

# Tartalom

# Az Információ Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy a Szervezet üzleti tevékenységének gyakorlása során biztosítsa az adatkezelés, adatvédelem elveinek, az adatbiztonság, informatikai biztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést.

Az IBSZ célja továbbá:

- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az adatállományok biztonságos mentése,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembehelyezésen keresztül az üzemeltetésig.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

**Alkalmazott jogszabályok és iránymutatások**

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- az Európai Parlament és Tanács (EU)2016/679 rendelete (GDPR)
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- ISO 27001 és ISO 27002 minősítésekkel kapcsolatos elvárások
- NAIH-4188-2/2012/V NAIH határozat

**Az IBSZ személyi hatálya**

Jelen szabályzat kiterjed a Szervezet munkavállalóira, munkavégzésre irányuló egyéb jogviszonyban állókra és külön megállapodás alapján alvállalkozóira.

**Az IBSZ tárgyi hatálya**

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülési és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed a vállalkozás tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

**Az IBSZ időbeli hatálya**

A szabályzatot bármilyen szerződéses jogviszony keletkezésétől annak fennálltáig kell alkalmazni.

A munkavállalók munkaszerződésük, a munkavégzésre irányuló egyéb jogviszonyban állók a megbízási szerződésük aláírását követően bevezető képzésen vesznek részt, amelynek kötelező részét képezi az IBSZ ismertetése, az abban foglaltak elfogadása, betartása. A képzésen történő részvételt a munkavállaók és a munkavégzésre irányuló egyéb jogviszonyban állók a jelenléti ív aláírásával igazolnak.

Ha az alvállalkozói szerződés személyes adatok kezelésére is kiterjed, úgy az alvállalkozó köteles gondoskodni a képzésben történő részvételről.

A kötelező képzést az IBSZ az éves kötelező felülvizsgálatot, illetve az eseti módosításokat követően meg kell ismételni, ennek megszervezése a társaság ügyvezetőségének kötelezettsége.

A Szervezettel bármilyen szerződéses viszonyban állót titoktartási kötelezettség terheli. A Szervezet titoktartási nyilatkozat aláírására a munka-, megbízási és alvállalkozói szerződés aláírásával egyidejűleg kerül sor.

A Szervezet évente legalább egy alkalommal tájékoztatót tart a tevékenységgel kapcsolatos biztonsági követelményekről.
A vállalat az információbiztonsági tudatosság szintjének folyamatos emelése érdekében rendszeres képzésekben részesíti munkatársait legfeljebb éves gyakorisággal. A munkatársak ezen a képzéseken és a hozzájuk kapcsolódó vizsgákon (értékeléseken, teszteken) kötelesek részt venni és legalább megfelelő eredményt elérni.

Aki tartósan nem teljesíti az oktatási követelményeket az a munkaköre betöltésére alkalmatlanná válik.

A képzéseket a Vezető tervezi meg. A képzések tárgyköre át kell fogja az alábbiakat:

- információbiztonsági ismeretek
- adatvédelmi ismeretek,
- érvényes szabályozások, előírások

Az információbiztonsági tudatosság ellenőrzése a képzésekhez kapcsolódó vizsgákon, és a tervezett felmérések, versenyek, kampányok, valamint az információbiztonsági auditok során valósul meg.

**Információbiztonsági Szerepek és felelősségek**

Az információbiztonsággal kapcsolatos felelősség megoszlik az Vállalat vezetősége, a Megbízott Rendszergazda, valamint az egyes munkavállalók és megbízási szerződéssel megbízottak (együttesen munkatársak) között. A felelősség megosztás elveit az alábbiakban tárgyaljuk.

A felső szintű felelősség az információbiztonság folyamatos biztosításáért, az információbiztonsággal kapcsolatos szabályozásokért, a vállalati információbiztonsági tudatosság megfelelő szintjének biztosításáért, az információbiztonsággal kapcsolatos vállalati célkitűzésekért, valamint az információbiztonsági intézkedések bevezetéséért a Megbízott Rendszergazda személyénél összpontosul.

Az információbiztonság koordinálásának felső szintű vezetője a Vezető.

Ezen felül minden szervezeti egység vezetője személyesen felel az információbiztonság fenntartásáért. A vezetők elkötelezettségüket személyes példamutatással (pl.: szabályozások betartása) és személyes felelősségvállalással demonstrálják.

**Feladatkörök szétválasztása**

Szervezetnél a következő Információbiztonsági felelősségi körök definiáltak:

- A Kft Ügyvezetője (továbbiakban Vezető)
- a Szervezet által Megbízott Rendszergazda
- Adatvédelmi Tisztviselő

A Vezető főbb feladatai:

- Az Információbiztonsági Rendszerrel kapcsolatos információk egyeztetése a Szervezet Megbízott Rendszergazdájával,
- Az Információbiztonsági rendszer működéséhez szükséges erőforrások biztosítása,
- Az Információ Biztonsági rendszer belső és külső auditálására megbízás adása.

Szervezet Megbízott Rendszergazdájának főbb feladatai:

- Az Információbiztonsági rendszer bevezetése, működtetése, a folyamatos fejlesztése, illetve az eredményesség fenntartása
- Jogosultságok kezelése,
- adatmentések felügyelete és naplózása,
- Informatikai rendszer teljesítményének mérése,
- telepített szoftverek átvizsgálása,
- rendszernaplók, víruskeresési naplók , egyéb naplók figyelése,
- az eszközök megfelelő működésének ellenőrzése,
- hálózati működéshez szükséges szoftverek telepítése és beállítása,
- az általános átvizsgálás során észlelt hibák javítása,
- megelőző lépések megtétele,
- munkatársak bejelentései során incidensek monitorozása és javítása ,
- a munkatársak igényeinek figyelemmel kísérése,
- javaslatok összeállítása a meglévő szoftverek felhasználására,
- új szoftverek beszerzésére javaslattétel,
- biztonsági beállítások folyamatos felülvizsgálata és szükség esetén korrigálásuk,
- új eszközök vásárlásához javaslatok megtétele,
- A Szervezet információs adatvagyonának felmérése és a nyilvántartás karbantartása
- szerverek telepítése, üzemeltetése.
- szerver oldali virtualizációs környezet üzemeltetése, karbantartása,
- hálózati tűzfal menedzsmentje,
- második szintű támogatás.

Adatvédelmi Tisztviselő főbb feladatai:

- adatvédelmi incidensek jelentése
- az Adatvédelmi Tisztviselő részletes feladatait a Szervezet Adatvédelmi Szabályzata tartalmazza

**Kapcsolat a hatóságokkal és szakmai csoportokkal**

Az információbiztonsági (adatvédelmi) incidensek esetén a Megbízott Rendszergazda és az Adatvédelmi Tisztviselő kötelessége:

- az esemény jelentése, a jelentés elkészítése,
- a kapcsolódó bizonyítékok átadása,
- együttműködés a vizsgálatok lefolytatásában.

A hatóságoknak jelentendő incidenseket a Vezető határozza meg. A Megbízott Rendszergazda ezt a feladatát a Szervezet jó hírének és érdekeinek védelmének szem előtt tartásával végzi.

Az információbiztonságot érintő ügyekben a Szervezet Megbízott Rendszergazdája köteles kapcsolatot tartani és információt szolgáltatni a következő szervezetek/személyek irányába: Rendőrség, Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Adatvédelmi Tisztviselő.

A Megbízott Rendszergazda folyamatos kapcsolatot ápol a Szervezet vezetőségével, valamint szükség esetén szakértői információbiztonsági tanácsadást vesz igénybe az információbiztonsági politika, és kapcsolódó szabályozások érvényesítése, az információbiztonság fejlesztésével kapcsolatban és az információbiztonsággal kapcsolatos ismeretek folyamatos frissítése érdekében.

Külső support szolgáltató köteles késedelem nélkül jelezni minden rendellenes vagy annak vélt eseményt az egyéb rendszergazda szolgáltatással megbízott szervezetek, a Vezető és az Adatvédelmi Tisztviselő felé.

A Szervezet nem rendelkezik belső rendszergazdával, így a rendszergazdai feladatok ellátására külső vállalkozókat bíz meg. A feladatok ellátásával kapcsolatban a Szervezet adatfeldolgozói szerződést köt a külső szolgáltatókkal.

Jelen IBSZ-ben említett „Megbízott Rendszergazda" hivatkozások minden esetben az adott Megbízott Rendszergazda saját hatáskörébe tartozó rendszerekre vonatkoznak.

Az emberi erőforrások biztonsága a Szervezet vezetősége elkötelezett az információbiztonság szervezeten belüli növelése érdekében.

Az információbiztonsági kockázatok között kiemelt helyet foglalnak el a munkavállalókkal kapcsolatos kockázatok, mivel a munkavállalók a munkavégzésük során hozzáférhetnek a Vállalat számára bizalmas és titkos adatokhoz, dokumentumokhoz, amelyekkel esetlegesen visszaélve, vagy akár csak gondatlanul kezelve azokat, súlyos károkat okozhatnak.

Éppen ezért információbiztonsági előírásainak megfelelőn a Szervezet különös gondot fordít a munkavállalókkal kapcsolatos kockázatok kezelésére a munkavállalók alkalmazása előtt, alatt, valamint az alkalmazás megszűnése, vagy az alkalmazási feltételekben történő változások eseteiben.

Az alkalmazottakat, szerződéses viszonyban alkalmazott feleket úgy kell kiválasztani, munkaköri feladat és felelősségi köreiket úgy kell kialakítani, hogy tisztában legyenek felelősségükkel, alkalmasak legyenek feladataik biztonságos ellátására és egyúttal a lopás, a csalás és a visszaélés kockázatát is csökkentsük.

**A munkaviszonnyal kapcsolatos feltételek és kikötések**

Társaságunknál az információbiztonsági vagy azzal összefüggő célok elérése érdekében az új belépőknek az alábbi dokumentumokat kell megismerniük, és az alábbi nyilatkozatokat, megállapodásokat kell aláírásukkal igazoltan elfogadniuk:

- Tűz- és Munkavédelmi szabályzat
- Fegyelmi szabályzat
- Információbiztonsági szabályzat
- Az adott munkakörre vonatkozó speciális elvárások szabályzata
- Üzletmenetfolytonossági Terv
- Adatvédelmi Szabályzat

Aláírandó nyilatkozatok, megállapodások:

- Titoktartási nyilatkozat
- Nyilatkozat az elolvasott dokumentumokról
- Adatkezelési tájékoztató megismeréséről szóló illetve hozzájáruló nyilatkozat

**A munkaviszony megszűnése és megváltozása**

A foglalkoztatás megszűntetésére javaslatot a közvetlen vezetők tesznek a munkaviszony létesítéséhez, illetve megszüntetéséhez kapcsolódó munkáltatói jogok gyakorlójának. Az alkalmazás megszűntetéséről a munkaviszony létesítéséhez illetve megszüntetéséhez kapcsolódó munkáltatói jogok gyakorlója dönt.

Az alkalmazás megszűnését követő meghatározott időszakig történő titoktartást a munkatársaktól az alkalmazás megkezdésekor kitöltött titoktartási nyilatkozatban kell rögzíteni.

Az alkalmazás megszűnésekor a kilépő munkatársak kötelesek minden, a Szervezet tulajdonát képező vagyontárgyat visszaszolgáltatni. Ennek ellenőrzése érdekében a munkaáltató jogosult a munkavállalóra bízott vagyontárgyakat soron kívül leltározással ellenőrizni. A hiányokat vagy károkat a munkatárs köteles megtéríteni, az adott vagyontárgy könyv szerinti értéke alapján. Meg kell róla győződni, hogy minden a

munkatárs nevén szereplő vagyontárgy az eszközgazdálkodás és a konfiguráció kezelés nyilvántartásaiban (cél) visszavételre, vagy új tulajdonoshoz rendelésre kerüljön.

A munkatárs jogosult a visszaszolgáltatott vagyontárgyakról a személyes adatait eltávolítani, de nem jogosult a Szervezet tulajdonát képező információkat törölni.

A kilépő munkatárs köteles a privát eszközeiről (Mobil telefon, laptop, pendrive...stb.) a vezetője vagy a kiléptetést végző személy jelenlétében eltávolítani minden hozzáférést, Szervezeti anyagot különös tekintettel a mobil eszközök által nem fizikai eszközökre szinkronizált dokumentumokat.

Az összes hozzáférési jogot az alkalmazás megszüntetése, változtatása után meg kell szüntetni, mely feladatot a Megbízott Rendszergazda látja el.

Minden vezető felelős az általa vezetett munkatársak munkaviszonyának megszűnését követően a Szervezeti rendszerekben adott jogosultságok visszavonásáról meggyőződni, hiba esetén intézkedést kezdeményezni.

A távozó munkatárs vezetője felelős a távozással érintett szerepkörök folytonosságát biztosítani, az új munkatársat kijelölni.

A Megbízott Rendszergazda évente rendszeresen ellenőrzi a megszűnt munkaviszonyú munkatársak jogosultságainak visszavonását a belső audit keretében a rendelkezésére bocsátott névsor alapján, és a jogosultságokat köteles vezetni a „Jogosultsági mátrixban".

Abban az esetben, ha egy Szervezettől távozó dolgozó jogosultságainak létezését vezetője kockázatosnak ítéli meg a következők szerint kell eljárni:

Mielőtt a dolgozóval vezetője közli az elbocsátást a közvetlen vezetőjét tájékoztatni kell az elbocsátás bejelentésének pontos időpontjáról, a várható visszavonási igényekről, valamint elő kell készíteni a dolgozó céges eszközeinek elvételét.

Az elbocsátás közlésével egy időben azonnal végre kell hajtani a következőket:

- Desktop vagy laptop visszavételezése
- Mobil eszközök visszavétele

Az elbocsátás tényének közlése után a kísérő személy és a dolgozó felettese visszakíséri a dolgozót a munkavégzés helyére, ahol lehetősége van összeszedni a személyes tárgyait majd a céges eszközök átadása után a dolgozót kikísérik az épületből.

A Megbízott Rendszergazda köteles a visszavett adathordozóknak teljes törlésére/formatálására illetve a távozott kolléga postafiókjának megszüntetésére és tartalmának törlésére. Amennyiben a távozó munkatárs kulcsszerepet játszott bizonyos folyamatok kapcsán, az email címe a távozást követő három hónapban megmaradhat és egy automatikus válasszal jelezhető a küldő félnek, hogy a jövőben kinek címezheti a megadott tartalmú emaileket.

**Szabály a hozzáférés felügyelethez**

A jogosultságok kiosztásának alapelve, hogy mindenki a munkájának elvégzéséhez szükséges információkhoz a feladatának megfelelő módon tudjon hozzáférni, de sem ennél több, sem ettől eltérő típusú hozzáféréssel ne rendelkezzen, valamint minden feleslegessé vált jogosultságot késedelem nélkül megszüntessenek. A jogosultságok kiosztását, azaz a jogosultság kezelés folyamatát úgy kell megoldani, hogy a munkavégzéshez szükséges alapvető jogosultságok mindig rendelkezésre álljanak minden feladatkörben, és az ezt meghaladó igényeket megfelelő jóváhagyási folyamaton át ellenőrzött módon zökkenőmentesen lehessen teljesíteni. A jogosultság kezelési folyamatnak biztosítania kell a kiosztott jogosultságok ellenőrizhetőségét, és a visszavonás hiánytalan megtörténtét.

A szabályozás naprakészen tartása a Megbízott Rendszergazda és a Vezető feladata. A szabályozásban foglaltak szerinti működés feltételeinek biztosítása a Vezető felelőssége.

A Szervezet belső hálózatához kívülről (nem Szervezet által felügyelt hálózatból) az arra jogosultságot kapott felhasználók, csak az Szervezet által biztosított VPN kapcsolaton át csatlakozhatnak. Szigorúan TILOS bármiféle ettől eltérő megoldás megkísérlése a felhasználók részéről.

A Szervezet belső hálózatához csak a Szervezet ellenőrzése alatt álló eszközöket szabad csatlakoztatni.

Külső cégeknek tilos a berendezéseiket a Szervezeti hálózaton külön engedélyezés nélkül üzemeltetniük.

Minden, a belső hálózatra csatlakozó berendezést azonosítani kell tudni. A belső hálózathoz csak az arra jogosult, azonosított eszközök csatlakozhatnak. A csatlakozás ellenőrzésére és a csatlakozott eszköz azonosítására a 802.1x authentikációs eljárást kell használni. Az eljárás használatához szükséges biztonsági tanúsítványok létrehozása a Szervezet szerverén történik, és az illetékes üzemeltető feladata a hálózathoz kapcsolható engedélyezett eszközökre történő telepítése.

A fenti megkötések alól kivételt képeznek a vendég WiFi csatlakozási lehetőségek, amik a vendégek számára biztosítanak Internet elérést. Ezek a csatlakozások úgy kerülnek kialakításra, hogy azokról a Szervezet belső hálózatán található szolgáltatások semmiképpen nem lehetnek elérhetők. A mobil (főként privát) eszközei szintén csak a vendég WiFi hálózathoz csatlakozhatnak.

**Külső szereplőkkel való együttműködés**

Külső szereplőnek (partnernek) minősül minden olyan intézmény, vállalat, vállalkozás vagy egyén, aki valamely formában (hatóságként, társadalmi szervezetként, szolgáltatóként, alvállalkozóként, ügyfélként, stb.) együttműködik a Szervezettel, beszállít a Szervezetnek, illetve akinek szállít valamit a Szervezet. Ezen tevékenység nem kívánt kockázatokat rejt(het) magában, amelyeket szükséges kezelni, szabályait és irányelveit összefoglalni, mellyel a külső partnerek számára biztosított információhoz való hozzáférések információbiztonsági kockázatai kezelhetők, illetve csökkenthetők.

Vendégek tartós jelenléte esetén, az asztalokon érzékeny üzleti információkat tartalmazó dokumentumok tárolásának elkerülése indokolt és a vendégek csak kísérettel léphetnek be az irodahelyiségekbe.

A vendégek a fénymásoló eszközöket csak felügyelettel használhassák. A kiemelten fontos területekre vendégek csak abban az esetben léphessenek be, ha egy illetékes munkatárs kíséri őket a helyiségbe.

A vendégek számára az első belépési pontot a portaszolgálat jelenti, ahol nem készítenek feljegyzéseket az érkezőkről. A Szervezetbelépőkártyákat alkalmaz, amelyek egyedi azonosítóval ellátottak, és csak az alkalmazottak részére kerülnek kiadásra. A kártya elvesztése/eltulajdonítása esetén a munkatársak kötelesek a Szervezet vezetőjét azonnali hatállyal tájékoztatni, aki megteszi a szükséges intézkedéseket a jogosulatlan behatolás elkerülése érdekében.

**Felhasználók regisztrálása és törlése**

Regisztrálás:

A felhasználókat egyedi felhasználónévvel kell azonosítani. Csoportos felhasználóneveket TILOS használni. A felhasználók azonosítása a mindenkori névkonvenció szerint egyedi, a felhasználó nevéből képzett azonosítók használatával történik.

A névkonvenció szabálya: Keresztnév kezdőbetűje majd a Vezetéknév ékezet jelek és szóközök nélkül ponttal elválasztva. Ugyanazon nevű munkavállalók esetében a Vezetéknév után növekvő sorszámmal (2-től induló számozás) került megkülönböztetésre.

Új felhasználó regisztrálásának előfeltétele az aláírt munkaszerződés. Ennek hiányában csak a Vezető engedélyével regisztrálható új felhasználó a Szervezetnél.
A felhasználók regisztrálása és a felhasználói adatok módosítása a Megbízott Rendszergazda feladata. Az említett munkautasítások naprakészségéért a Vezető felelős.

Felhasználó törlése:

Munkavállaló kilépése esetén a folyamatot elindításáért a munkavállaló közvetlen vezetője a felelős. A felhasználó törlésére a Megbízott Rendszergazda jogosult a Vezető írásbeli utasítása alapján.

A bejelentő vezető ezzel egyidejűleg – ha a kockázatok indokolják – soron kívül teszi meg a szükséges további információvédelmi intézkedéseket is. (pl. visszaélés gyanúja esetén soron kívüli felfüggesztés elrendelése stb.)

**Felhasználói hozzáférés biztosítása**

A jogosultságkezelési folyamatban az alábbi általános szabályok az irányadók:

- Hozzáférést csak a szükséges mértékben és időtartamra szabad engedélyezni, olyan személyek számára, akiknek a feladataik ellátása és/vagy jogaik gyakorlása érdekében indokolt. A szükséges mértékre és időtartamra történő korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelősséget is.
- A Szervezet rendszereihez csak a jogosultságkezelési folyamat betartásával adható hozzáférés.
- Külső partnerek (vállalkozók stb.) vonatkozásában a Szervezet IT rendszereihez való hozzáférés csak szerződés alapján biztosítható.
- A vállalat IT rendszereihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés, megállapodás vagy titoktartási nyilatkozatok alapján gyakorolhatják.
- A hozzáférési jogosultságokkal történő visszaélés gyanúja esetén a Szervezet minden dolgozója köteles értesíteni a Vezetőt és az Adatvédelmi Tisztviselőt.
- Jelen szabályzattól eltérni a Vezető engedélye esetén lehetséges. (Ilyen esetekben is szükséges a folyamat megfelelő dokumentálása)

A Szervezetnél a következő alapjogosultságok illetik meg a dolgozókat

- Szervezet Domain név
- Szervezet levelezés
- Internet elérés belső hálózaton keresztül
- Belső hálózat elérése (a munkakörhöz szükséges meghajtókhoz és mappákhoz)
- Eszköz elindításához szükséges kezdeti jelszó.

Ezen kívül dedikált jogosultság jár, ha egy adott csoport tevékenysége alapján szükséges, előre meghatározott jogosultságok, amelyeket személyre szólóan kell igényelni. Ide tartoznak az alapjogosultságokon felüli, a Szervezet rendszereihez való hozzáférések (pl. számlázó program, követeléskezelő szoftver, stb.).

**Privilegizált jogosultságok (rendszergazdai jogosultságok)**

Minden olyan jogosultság ebbe a körbe tartozik, amely a felhasználói jogoknál több jogot jelent (pl. rendszeradminisztrátor stb.). Főbb szabályok a privilegizált jogosultságokkal kapcsolatban:

A rendszerek adminisztrációjához kellő rendszergazdai jogosultságot (előjogokat) csak a rendszergazdai feladatkörben foglalkoztatott munkatársak kaphatnak és csak a feladatkörüknek megfelelő rendszerekre érvényesen. A rendszergazdai jogosultságok (előjogok), ahol ennek kifejezett műszaki akadálya nincsen, legyenek egyértelműen személyhez kötöttek, a csoportos azonosítók használata mindenképpen kerülendő.

A rendszergazdák az előjogokat biztosító azonosítójukat csak a munkavégzéshez feltétlenül szükséges mértékben használják, minden más esetben a normál felhasználói azonosítójukkal dolgozzanak.

Mindenképpen kerülni kell olyan rendszerek üzembe állítását, amelyek nem rendszergazda munkakörben dolgozó felhasználók rendszergazdai jogosultságokkal történő felruházását igényelnék.

**Felhasználók titkos hitelesítési információnak kezelése**

Minden munkaállomás egy egyedi jelszóval van védve, a kezdeti jelszót átadjuk a munkavállalónak, aki az első bejelentkezés során köteles megváltoztatni azt.

Amennyiben a munkavállaló elveszíti a jelszavát, a Megbízott Rendszergazda visszaállítja a kezdeti jelszavát, majd a munkavállaló első bejelentkezéskor ismét köteles megváltoztatni azt.

Minden munkaállomás a Windows beépített Bitlocker megoldásával kerül titkosításra (nem PIN kód alapú, így a munkaállomás indításakor nem igényel felhasználói beavatkozást), melynek feloldó kulcsait a Szervezet trezorjában őrizzük és a Megbízott Rendszergazda nem tárol arról másolatot.

**Felhasználói hozzáférési jogok átvizsgálása**

A felhasználó által igényelt jogosultságok indokoltságát és információbiztonsági megfelelőségét a munkahelyi vezetőnek és az adatgazdának kell rendszeresen (évente legalább egyszer) átvizsgálnia.

A már regisztrált felhasználók adatainak helyességét és a részükre megadott jogosultságokat rendszeresen, legalább évente egy alkalommal át kell vizsgálni, azzal a céllal, hogy az adminisztráció során bekövetkezett hibákat/tévedéseket kiszűrjék.

Ellenőrizni kell az adatok helyességét, ki kell szűrni

- a már kilépett, de esetleg a rendszerben bennmaradt munkatársakat,
- a megváltozott munkakör után megmaradt régi jogosultságokat,
- az ideiglenesen megadott, már lejárt jogosultságokat.

Az átvizsgálásnak kezdeményezése a Vezető felelőssége és a Megbízott Rendszergazda hajtja végre.

**A hozzáférési jogok visszavonása vagy módosítása**

A hozzáférési jogosultságok megszüntetéséről (teljes visszavonásáról) a felhasználó közvetlen vezetője az alábbi esetekben köteles intézkedni és felelősséggel eljárni:

- dolgozó kilépése esetén,
- ha a munkavállaló szervezeti egységen belül marad, de a munkaköre jelentősen megváltozott
- ha a külső partner szerződése lejárt vagy megszűnt,
- tartós (3 hónapon túli) betegség, távollét, illetve helyettesítés esetén,
- tartós (3 hónapon túli) kirendelés esetén,
- visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.

Bármely - a munkavállaló kilépésén kívül - a jogosultsági igényekben bekövetkező változás miatt szükségessé váló jogosultság visszavonása esetén a Vezető írásos értesítése szükséges.

IT rendszerek közötti kapcsolat megszüntetését vagy felfüggesztését a Megbízott Rendszergazda kezdeményezheti a Vezető írásos utasítása alapján.

**Titkos hitelesítési információk használata**

Minden Szervezet dolgozó a hozzá tartozó titkos hitelesítő információkat bizalmasan kezeli, egy munkatárssal sem oszthatja meg. Papír alapon nem tárolhatja sem a munkahelyén, sem otthonában.

Gondatlan hitelesítési információ használatból fakadó károkért a dolgozó vállal felelősséget, melynek részletei a Szervezet Adatvédelmi Szabályzatában kerültek tisztázásra.

Ezen információk csak a Vezető írásos engedélyével osztható meg. Amennyiben külső szolgáltatóktól kell jogosultságot szerezni a Szervezet munkatársának, a Rendszergazda az adott területi vezetővel együttműködve végezheti ezt a tevékenységet.

A felhasználók számára szigorúan TILOS privát felhasználású felhő szolgáltatást alkalmazni az üzleti adatok tárolására. Ezen privát eszközök közé tartoznak a felhasználók személyes email fiókjai is.

**Felhasználói jogosultságok nyilvántartása**
A Megbízott Rendszergazda és a Vezető felelőssége az IBSZ 3. mellékletét képző „Jogosultsági mátrix" napra készen tartása.

**Biztonságos bejelentkezési eljárások**

- Jelen szabályzat a jelszókezelésre vonatkozó rendelkezés, melynek célja meghatározni a Szervezet IT rendszereihez hozzáférést biztosító jelszavak és felhasználói nevek kezelését, képzését, módosítását, valamint az IT rendszerek jelszókezelő alrendszerének egységes követelményeit.
- A jelszó az egyik fő eszköz arra, hogy a felhasználó az IT rendszerekhez való hozzáférési jogosultságát érvényesítse, és az illetéktelen hozzáférést meggátolják. Főbb szabályok a jelszó használat kapcsán:
- A jelszó jogosulatlan személynek történő átadása vagy hozzáférhetővé tétele üzleti titoksértésnek minősül, ami munkajogi és büntetőjogi felelősségre vonás alapját képezheti.
- A felhasználóknak a jelszavaikat bizalmasan kell kezelniük, azt senkivel nem közölhetik. A jelszó közlését senki nem kérheti a felhasználótól.
- Egy adott IT rendszerben minden felhasználó számára egyedi felhasználói azonosító és ehhez rendelt jelszó alkalmazása kötelező. Csoportos jelszó és felhasználói azonosító használata tilos!
- A felhasználók a jelszavaikat csak abban az esetben jegyezhetik fel, ha a Vezető által erre a célra meghatározott, engedélyezett eszközzel és módon történik.
- Valamennyi új hozzáférésnél minőségi induló jelszó megadása kötelező, melyet az felhasználónak, kikényszerített módon azonnal, az első használat alkalmával, a kiadást követően legfeljebb egy napon belül, le kell cserélnie saját jelszavára.
- Az átadás során a kezdeti jelszó bizalmasságának megőrzését és az illetéktelen hozzáféréstől történő megóvását zárt boríték használatával kell biztosítani.
- Az felhasználó személyazonosságának megbízható megállapítása a borítékot személyesen átadó Vezető feladata.
- A rendszergazdáknak TILOS a felhasználó kérése alapján jelszót beállítaniuk, a jelszót minden esetben a felhasználónak kell magának beállítania.
- A jelszavakat nyílt szöveg formájában TILOS tárolni vagy bármilyen csatornán továbbítani.
- Jelszavak begépelése során a billentyűzetet illetéktelen személyek rálátásától védeni kell.
- A Szervezet rendszereiben használt jelszóval azonosat TILOS más, például nyilvános vagy otthoni rendszerekben használni.
- Ha a felhasználó jelszavának visszaállítása válik szükségessé, akkor a jelszó visszaállítása előtt meg kell győződni a visszaállítást igénylő felhasználó személyazonosságáról. Ideiglenes, egyszeri bejelentkezésre használható jelszót kell kiadni a kezdeti jelszó kiadásával azonos követelmények szerint.

A nem megszemélyesíthető felhasználók (például rendszeralkalmazások) részére is legalább a jelen szabályzatban meghatározott minőségi jelszavakat kell megadni.

A Szervezet IT rendszereiben csak minőségi jelszó használható. A minőségi jelszó képzésének szabályai az alábbiak:

- Minimálisan 12 alfanumerikus karakterből áll.
- A legutóbbi 5 jelszó használata nem megengedett.
- Amennyiben az adott IT rendszer támogatja, írásjeleket és speciális karaktereket is tartalmaz, pl. ( ),.?+.
- Csak ékezetmentes betűből áll.
- A jelszó nem lehet azonos a felhasználói azonosítóval.
- A jelszó legyen összetett, a négy típusú karakterből (kisbetű, nagybetű, szám, speciális jelek) legalább három típus szerepeljen a benne.
- Nem tartalmazhat azonos karakterből, vagy egymás után következő számból, betűből, vagy a billentyűzeten egymást követő karakterekből álló csoportokat (karaktercsoportnak számít 3 egymást követő karakter),
- Semmi olyat nem tartalmazhat, amelyet bárki más könnyen kitalálhat, vagy az illető személyével kapcsolatos adatokból kinyerhet, például nevekből, telefonszámokból, születési adatokból stb.
- A jelszó módosításánál az új jelszó kialakításánál törekedni kell arra, hogy szerkezetében ne hasonlítson az előző, lecserélendő jelszóra.
- A jelszó lejárata legfeljebb 90 nap.
- A vállalat minden munkatársa számára személyes jelszó kezelő rendszer biztosított, ahol minőségi jelszó generálható, amelyet utána ebben a rendszerben tárolni is lehetséges.
- A minőségi jelszó generálása a munkatársak számára biztosított illetve a vendég WIFI hálózatok jelszó generálása esetén is érvényes.
- A jelszavakat legalább 90 naponként meg kelljen változtatni.
- A kezdeti jelszót az első használat során kénytelen legyen a felhasználó megváltoztatni.

A Szervezet jelszókezelő alrendszere biztosítja a rendszer alapvédelmét, azt, hogy csak a jogosult felhasználó férhessen hozzá - egy sikeres bejelentkezési folyamat után - az IT rendszerben tárolt adatokhoz.

A felhasználók bejelentkezésének azonosítása és hitelesítése tárolt azonosítók alapján kell történjen. Csak ezután legyen lehetséges az esetlegesen további, felhasználó kezelést tartalmazó rendszerekbe történő továbblépés.

A felhasználók a külön felsorolt erős authentikációt igénylő eseteken kívül egyszerű authentikációval, felhasználónév és jelszó megadásával kerülnek azonosításra és hitelesítésre.

Az erős authentikációt igénylő esetek: VPN használat, rendszergazdák távoli hozzáférése.

A jelszókezelő rendszert úgy kell kialakítani és beállítani, hogy a jelszavak jó minőségét és biztonságos használatát biztosítsa.

**Szabály a titkosítási intézkedések kapcsán**

A Szervezetnél minden adat szerveren kerül tárolásra, melyről naponta biztonsági másolat is készül. A szervert a Szervezet által választott titkosítási algoritmus védi a fizikai és szoftver alapú támadásoktól is.

A szerverek fizikai eltulajdonítása után sem érhetőek el a tárolt adatok a fent említett titkosítási folyamatnak köszönhetően.

A titkosítás automatikusan történik, a rendszer működésének megfelelősségét a Megbízott Rendszergazda végzi meghatározott rendszerességgel.

A Szervezet által alkalmazott honlapoknak illetve webes alkalmazásoknak minden esetben rendelkezniük kell biztonságos HTTP kapcsolattal (HTTPS) valamint a honalap adatbázisának titkosítása szükséges (amennyiben létezik). A honlapokon minden esetben elérhető teszi a Szervezet az adatkezelési és cookie tájékoztatóját.

A Szervezet munkatársai által használt eszközöket a használatba vétel előtt titkosítási intézkedéssel látja el a Szervezet Megbízott Rendszergazdája.

A Szervezet gondoskodik a központi szervereken tárolt információk (pl.: adatbázisok, jelszavak) titkosításáról is. A kulcsfontosságú eszközök titkosító kulcsát a Vezető ismeri, melyek digitális és papír alapon a vállalat trezorjában kerülnek elhelyezésre.

**Tiszta asztal és tiszta képernyő szabálya**

Az irodahelységekben az íróasztalokon rendet kell tartani. Csak a munkához felhasznált iratok, adathordozók lehetnek az asztalokon munkaidőben. Munkavégzés után, vagy ha nem tartózkodik senki a helyiségben, az íróasztalokról az adathordozókat, munkához felhasznált iratokat zárható szekrénybe el kell zárni.

A felhasználók kötelesek a munkájuk megszakítása vagy befejezése után a számítógépüket zárolni vagy kikapcsolni.

A munkatársak a munkához szükséges file-jaikat az arra kijelölt hálózati helyen kötelesek tárolni. A számítógép asztalán csakis az egyes alkalmazások parancsikonjai helyezhetőek el. A gyorsabb munkavégzés miatt a számítógépre másolt adatokat a dolgozó saját mappájában köteles tárolni a munkavégzés idejére, melyet ugyancsak köteles a hálózati adattárhelyre visszamásolni a munkamenet lezárását követően (a számítógépről pedig törölnie szükséges).

**Korlátozások a szoftvertelepítésre**

A Szervezet tulajdonában lévő eszközökre csak a Vezető vagy helyettese jóváhagyásával telepíthető fel applikáció.

Nem jogtiszta szoftver telepítése és alkalmazása minden körülmények között tilos.

A Szervezet munkaállomásokra az operációs rendszer és a munkaköröknek/felhasználási módnak megfelelő alkalmazás csomag, valamint a megfelelő biztonsági beállítások telepítése történik.

A Szervezet munkatársai nem rendelkeznek local admin jogosultsággal, így csak a Megbízott rendszergazda képes telepítéseket futtatni.

A Megbízott Rendszergazda felelőssége

- a mindenkori üzleti követelményeknek megfelelő,
- az információbiztonsági követelményeket teljesítő
- szoftver csomagok elkészítéséről gondoskodni és azokat a felhasználói munkaállomásokra telepíteni.

Azon területeken, beosztásokban, ahol a munkafeladatok ellátása ezt elengedhetetlenné teszi, ott a Vezető külön engedélye alapján megengedett, a Szoftver Katalógustól eltérő, egyedi software környezet kialakítása, például más, vagy többféle operációs rendszer alkalmazása. Az ilyen eltérő szoftver környezet használatát csak abban jártas, megfelelően szakképzett munkatársak részére lehet megengedni. Ezen munkatársak maguk felelősek az általuk használt szoftver csomag biztonságos üzemeltetéséért.

**Internethasználat szabályozása**

A vírusvédelmi megoldások mellett a Szervezettartalomszűrést is alkalmaz a biztonságnövelése érdekében. A munkatársak által használt számítógépek esetén tartalomszűrést vezettünk be az alkalmazottak internetelérésének szabályozása érdekében, az alábbiak szerint:

- Kémprogramok, fertőző hordozható kódok és ártó tartalmak blokkolása mind web, mind messaging vonatkozásában
- Fájlcserélő (P2P) alkalmazások működésének megakadályozása

Instant Messaging szoftverek (pl: Facebook messenger) használatának tiltása és csatolmányaik blokkolása

## Szabály a mobil eszközök használatára

A munkavállaló részére használatba adott információ feldolgozó, továbbító és tároló eszközök (például laptop, mobil telefon, pendrive, stb.) valamint a mobil eszközökre biztosított informatikai szolgáltatások (például szoftver-alkalmazások, internet elérés, elektronikus üzenetküldés) a munkáltató tulajdonát képezik, annak felügyelete, ellenőrzése alatt állnak. Ezen rendszereket csak a munkavégzésre, a munkavégzés hatékonyságának javítására engedélyezett használni. A Megbízott Rendszergazda ellenőrizheti ezen eszközök és szolgáltatások szabályos rendeltetésszerű használatát.

- A munkáltató által a munkavállalónak biztosított mobil eszközt dokumentált átadás-átvételben kell rögzíteni.
- A rendelkezésre bocsátott informatikai infrastruktúrát a munkavállalónak rendeltetésszerűen kell használnia hardverek, mobil eszközökhöz biztosított szoftverek és szolgáltatások tekintetében egyaránt. A munkavállaló felelős az általa okozott károkat megtéríteni.
- Szigorúan tilos az információ feldolgozó rendszereket és hálózati szolgáltatásokat bármilyen jogsértő, vagy a Szervezet jó hírnevét veszélyeztető tevékenységre használni, azokon jogsértő vagy etikátlan tartalmakat tárolni továbbítani, vagy sokszorosítani. Tilos bármely jogszabályba ütköző tevékenységre bátorítás, bujtogatás, vagy akár csak ilyen tevékenységgel való egyetértés kifejezése.
- Szigorúan tilos adatok, információk jogosulatlan megszerzésére irányuló tevékenység, vagy annak kísérlete, üzleti, szolgálati titkok, vagy személyes adatok nyilvánosságra hozatala, más személy, vagy szervezet számítógépes szoftver vagy hardver elektronikus kommunikációja biztonsági rendszerének feltörése vagy annak kísérlete, tekintet nélkül arra, hogy a behatolás vagy a kísérlet adatok károsodását, adatvesztést, vagy más kárt okoz.
- A munkavállalónak tilos magáncélú eszközeit a munkahelyi számítógéphez vagy a Szervezeti hálózathoz csatlakoztatnia. Ez alól kivételt képez a Szervezeti levelező rendszer, amelyet csak úgy lehet mobil eszközre telepíteni, ha a készülék feloldásához és a rendszerbe való belépéshez jelszó szükséges.
- Tilos a munkahelyen engedély nélkül kép vagy hangfelvételt készíteni.
- A munkavállalónak a Megbízott Rendszergazda kivételével tilos az előre beállított biztonsági beállításokat engedély nélkül megváltoztatni.
- Ha a munkát bármilyen okból, bármilyen rövid időre is megszakítja, vagy befejezi, köteles a számítógépet kikapcsolni vagy zárolni, az iratokat elzárni (Clear desk elv).
- Megbízott Rendszergazda kötelessége minden visszavett eszközt teljes formázással törölni mielőtt új Munkatársnak adják ki
- A munkavállaló privát vagy a Szervezet által biztosított mobileszközein a kapcsolatokat csak a Szervezet által biztosított O365/email/Google/Apple fiókhoz szabad csatolni.
- A használati utasításokban a gyártó által megadott szabályokat mindig be kell tartani.
- A munka befejeztekor a mobil eszközt ki kell kapcsolni. Tilos a mobil eszközt bekapcsolva hagyni magáncélú internetes letöltés vagy távoli használat céljából.
- A helyi számítógépen vagy mobil eszközön történő munka során létrehozott dokumentumokat a lehető legrövidebb időn belül a megfelelő központi tároló eszközökön kell elhelyezni.
- Informatikai eszközök, adathordozók elvesztését, ellopását, megrongálódását haladéktalanul jelenteni kell a Megbízott Rendszergazdának.
- Informatikai eszközöket, adathordozókat TILOS nyilvános helyen őrizetlenül hagyni!
- Az informatikai eszközöket úgy kell elhelyezni, hogy a véletlenszerű rongálás (leesés, leverés, csepegő, fröccsenő folyadék) ellen minél védettebb helyen legyen.
- A gépek és rendszerek védelmére szolgáló jelszavak kiadása más munkavállalónak és külső félnek szigorúan TILOS! Ezek elvesztésének jelentése kötelező a Megbízott Rendszergazda és a Vezető felé az elvesztést vagy idegen kézbe kerülést követő 4 órán belül. Ennek elmulasztása fegyelmi eljárást von maga után.
- A távoli hozzáférést (VPN) biztosító tanúsítvány fájlok átadása és nem céges mobil eszközön történő tárolása szigorúan TILOS!
- Mobil eszközök nem használhatóak szimultán módon több hálózat (pld. védett VPN és publikus internet egyszerre) elérésére.
- Amennyiben nyilvános helyen használjuk a mobil eszközt (pld. hotel előcsarnok, internet kávéház, vonaton, hajón) jogosulatlan személyek belső céges információhoz férhetnek hozzá. Tilos ingyenes

és olyan WIFI hálózathoz csatlakozni, amelynek a forrása ismeretlen (pl: a szállodákban csak az a szálloda által biztosított és kellő azonosítással ellátott hálózatok használata engedélyezett)

- Tilos a saját mobil eszközzel ingyenes hot spotként megosztani internetet! A saját mobil eszköz hot spot védettségét biztosító jelszó elvárásait a Jelszókezelési szabályzatban foglaltaknak megfelelően kell beállítani.
- Céges adatok elérése a telephelyen kívül csak a Szervezet által rendelkezésre bocsátott eszközökkel (notebook, mobiltelefon) védett csatornán lehetséges (VPN)
- Céges autók kihangosító rendszerébe tilos szinkronizálni a kapcsolatokat (amennyiben ez szükséges, a Megbízott Rendszergazda köteles törölni azokat, mielőtt a cég használatán kívül kerül a jármű)

# Távmunka szabályzat

A rendszeres otthoni munkavégzés során olyan új információbiztonsági kockázatok merülnek fel, amik a normál munkahelyi környezetben hiányoznak, vagy az ott meglévő kockázatkezelő intézkedések sorának köszönhetően lényegesen kisebbek. Az lenne kívánatos, hogy az otthoni munkavégzés se legyen kockázatosabb, mint a munkahelyi. Ezeket a kockázatokat az otthoni munkahely speciális adottságainak megfelelően, a meglévő adottságok és a reális lehetőségek határain belül kezelni kell. Ez a szabályzat ezen kockázatok kezelése, a kockázatok elfogadható szintre csökkentése érdekében készült.

A szabályzat hatóköre: A Szervezet minden otthoni munkavégzést engedélyező és végző munkatársára érvényes.

Az otthoni munkavégzést a Vezető írásban engedélyezi. Az engedélyezés során megfontolás tárgyává kell tenni, hogy a munkavállaló

- személyisége,
- fegyelmezettsége
- információbiztonsági tudatossága
- és lakáskörülményei
- alkalmasak-e az otthoni munkavégzéssel járó kockázatok kezelésére.

Az engedély csak akkor adható meg, ha az otthoni munkavégzésre vonatkozó információbiztonsági szabályok betartásához szükséges feltételek rendelkezésre állnak.

A munkavégzés engedélyezéséhez kapcsolódóan minden esetben meg kell határozni,

- hogy a munkavállaló milyen munkafeladatokat végezhet el az otthoni munkahelyen,
- milyen egyébként a munkakörébe tartozó munkafeladatokat kifejezetten TILOS az otthoni munkahelyen végezni,
- milyen információkat (ezeket tartalmazó adathordozókat) szállíthat, tárolhat az otthoni munkahelyen.
- a kezelt információk bizalmasságát, az információ kiszivárgás kockázatát
- a kezelt információ rendelkezésre állásának kritikusságát (adatvesztés)
- az ügyfél szerződésekből és kapcsolódó jogszabályokból adódó korlátozásokat (jogi következmények)

Üzletileg indokolt esetben az otthoni munkavégzést engedélyező vezető saját felelősségére engedélyezheti az eltérést a jelen szabályzatban megadott követelményektől. Az eltérési engedélyt minden esetben írásba kell kiadni.

A számítógép védelme otthoni munkavégzés során:

- Az otthoni munkaeszköz kizárólag a Szervezet által biztosított számítógép lehet.
- Az eszköznek az alábbi tulajdonságokkal kell rendelkeznie
- a fokozott biztonsági fenyegetések ellen kellően védett, azaz
- titkosított adathordozóval ellátott, melyhez a hardware kulcsot vagy a PIN kódot a Szervezet rendelkezésre bocsájtja
- a hálózaton titkosítva kommunikáló, a Szervezeti hálózathoz VPN-en át kapcsolódó
- automatikusan frissülő vírusvédelemmel ellátott
- a képernyőt automatikusan lezáró kell legyen.

Az otthoni munkavégzésre alkalmas és a fenti követelményeknek megfelelő munkaeszköz biztosítása a munkáltató feladata. Az otthoni munkavégzés során az otthoni Wi-Fi hálózat jelszavának kellően biztonságosnak kell lennie, illetve használhatják közösen a környéken lakókkal.

## Szabályok és eljárások az információátvitelre

Az üzenetküldő szolgáltatások a Szervezet által a felhasználók részére privát eszközökön keresztül is elérhetőek. A felhasználónak biztosítania kell, hogy minden egyes bejelentkezés alkalmával (a Szervezet levelező rendszerbe) jelszóval azonosítania kell magát a privát eszközén.

A rendszer, valamint a rendszerben előállított, elküldött, továbbított, megkapott, tárolt vagy archivált üzenet a Szervezet felügyelete alatt áll, ezeket a Szervezet monitorozhatja, és tartalmába indokolt esetben szorosan a célhoz kötött módon betekinthet. Ilyen célok lehetnek: az üzletmenet folytonosság biztosítása, bizonyítékok gyűjtése információbiztonsági incidensek és fegyelmi ügyek kivizsgálásakor, valamint az erre jogszabályban feljogosított hatóságoktól érkező kérések teljesítése. A betekintés során megismert magántitok és személyes adatok kezelése csak a célhoz kötötten bizalmasan történhet.

A szolgáltatások nem használhatók személyes vagy magánjellegű üzenetváltás céljára, a Szervezet nem vállal felelősséget az ilyen tartalmú üzenetekben a személyes adatok védelméért.

A szolgáltatással mindennemű jogszabályellenes, vagy akár csak részben jogszabályba ütköző tartalom továbbítása és tárolása tilos, ideértve a szerzői jogi jogsértéseket is.

A felhasználó köteles biztosítani, hogy a tőle telhető legnagyobb diszkrécióval kezeli a Szervezeti információkat és az információbiztonsági elvek nem sérülnek a napi munkavégzés során, például amikor nem oldható meg egy megbeszélésen a prezentálás kiterjesztett képernyő segítségével, ki kell kapcsolnia az elektronikus üzenetküldő alkalmazást.

Elektronikus levelek továbbítása esetén fontos ügyelni arra is, hogy ne juttassunk át személyes adatot olyan felek között, akik nincsenek kapcsolatban egymással.

A levelezésben lévő különösen szenzitív csatolmányokat szükséges jelszavas védelemmel ellátni, illetve a csatolmány megnyitásához tartozó jelszót egy másik csatornán (pl.: SMS) eljuttatni a fogadó félhez.

A Megrendelő bizalmas információit a Szervezet alkalmazottai és vállalkozói nem beszélhetik meg telefonon vagy telefonkonferenciák keretében publikus helyszíneken, kivéve, ha minden résztvevő meggyőződött arról, hogy nincs a közelben illetéktelen személy, aki kihallgathatja a beszélgetést.

Az elektronikus üzenetküldő rendszer használata során nem megengedett:

- indokolatlanul nagy mennyiségű és méretű üzenetek küldése;
- reklámok és hirdetések közzététele;
- lánclevelek terjesztése, továbbítása;
- olyan üzenetek, illetve csatolt fájlok küldése, továbbítása, amelyek bármely módon történő jogszabálysértést vagy arra való felhívást tartalmaznak, sértik a Szervezet jó hírét.

A Szervezet minden tőle elvárható intézkedést megtesz az e-mail szolgáltatás megbízható és biztonságos üzemeltetése érdekében, de nem tud felelősséget vállalni egy üzenet elvesztése, késedelmes vagy hibás továbbítása okozta károkért. Ezért minden felhasználó köteles a kritikus fontosságú üzeneteinek célba érkezéséről magának meggyőződni. Erre a célra használható az olvasás visszaigazolás funkció, vagy szóbeli érdeklődés.

A felhasználó tudomásul kell vegye, hogy a Szervezetnek nem áll módjában a hálózatának határain túl az elküldött üzenetek továbbításának útvonalát felügyelet alatt tartani, azok biztonságáról gondoskodni. Ezért tilos az e-mail rendszeren át olyan tartalmú üzenetek küldése amiknek a megengedett továbbítási útvonalát törvényi rendelkezés, szerződéses kötelezettség, vagy belső utasítás előírja vagy korlátozza.

Az e-mail szolgáltatás során történő jelszó használatra is a Szervezet Jelszókezelési Szabályzatában megadott jelszóhasználati szabályok vonatkoznak.

Az e-mail rendszerben tárolt és továbbított dokumentumok kezelésénél is be kell tartani az érvényben lévő Iratkezelési szabályzatban leírtakat.

A Szervezet köteles gondoskodni a FTP megoldással továbbított adatok titkosított csatornán (SFTP) történő kezeléséről.

A Szervezet által küldött e-faxok esetében köteles a Szervezet a megőrzési időket figyelembe venni és a rendszerhez történő jogosultsásokat csak a jogosultak számára kiosztani.

**Elektronikus üzenetküldés**

A Szervezet nevében folytatott üzenetváltásban kizárólag az erre a célra biztosított elektronikus levelezési cím, a felhasználónak engedélyezett szolgáltatás használható. Más szervezet vagy szolgáltató által biztosított e-mail szolgáltatás üzleti céllal nem használható. Ezen szabálytól csak a Megbízott Rendszergazdától kapott egyedi engedély alapján lehet eltérni.

A felhasználó tudomásul kell vegye, hogy a leveleinek feladója, címzettje, és tárgya a technikai üzemeltetés során az üzemeltető személyzet részére látható lehet.

A felhasználó tudomásul kell vegye, hogy a munkaviszony megszűnése esetén a postafiókja a munkahelyi vezetője kérelme alapján archiválható, az abban található üzenetek az üzletmenet zökkenőmentes folytatása érdekében felhasználhatóak.

Minden esetben tiltott

- A Szervezet által biztosított e-mail címre érkező üzenetek átirányítása külső e-mail címre.
- a nem Szervezethez tartozó e-mail címre érkező üzenetek átirányítása a Szervezethez tartozó e-mail címekre.
- Ezen általános tiltások alól kivételes esetekben fontos üzleti érdekből a Megbízott Rendszergazda vagy a Vezető adhat felhatalmazást.
- A csatolmányokat minden esetben titkosítani vagy jelszóval ellátni szükséges.
- Emailek Szervezeten kívüli továbbítása során a beszélgetés előzményeit törölni kell.

VoIP alapú megoldások céges használata (különös tekintettel a csatolmányok továbbítására) TILOS!

Az általános információkezelési eljárásoknak megfelelően a bizalmas információkat e-mailben vagy annak csatolmányában csak titkosított módon szabad küldeni.

Bizalmas információt tartalmazó e-mailt vagy e-mailben kapott csatolmányt tilos a feladó kifejezett beleegyezése nélkül továbbítani.

Bizalmas információt tartalmazó üzenetet tilos levelezési listára küldeni.

Az információk kiszivárgása ellen védekezni kell. A védekezés elsődlegesen jelen szabályzat más pontjaiban felsorolt technikai intézkedések megvalósítása és viselkedési szabályok betartása révén valósul meg. Az információk kiszivárgását legjobban a munkatársak információbiztonság tudatos viselkedése akadályozhatja meg.

Minden munkatárs kötelessége, hogy a tudomására jutott, vagy a környezetében észlelt esetekben, az információbiztonságot veszélyeztető módon tevékenykedő, vagy viselkedő munkatársát figyelmeztesse, az esetet jelentse az Adatvédelmi Tisztviselő felé vagy a Vezetőnek.

Az információk kiszivárgása elleni védekezés érdekében a személyzet oktatásában tárgyalni kell az információbiztonsági fenyegetések aktuális trendjének témaköreit

- az információbiztonság tudatos általános viselkedési szabályok
- lehallgatás elleni védekezés
- social engineering elleni védekezés
- megtévesztés, félrevezetés elleni védekezés

A technikai védekezés keretében az alábbi megoldásokat alkalmazzuk:

- A munkaállomásokon, mobil számítógépeken és szervereken a rosszindulatú kódok elleni védelem része a bújtatott csatornákon át információt kiszivárogtató kém és trójai programok elleni védelem.
- Az információknak a mobil adathordozókon, faxon, email-ben, telefonon, vagy beszédben történő kiszivárgása ellen az információkezelési szabályokban megadott módon védekezünk. A védelem erősítését oktatásokkal és ismeret frissítésekkel valósítjuk meg.

Az asztali és mobil munkaállomásokon a mobil adathordozók ellenőrizetlen használatát korlátozó műszaki megoldásokat alkalmazunk.

# Vagyonelemek kezelése

A fejezet célja a Szervezet tárgyi eszközök kezelésével kapcsolatos szabályok és felelősségek meghatározása az egységes és átlátható, valamint eredményes eszközkezelés és eszközgazdálkodás megteremtése érdekében.

**Vagyonleltár**

A vezetés meghatározza a védendő információs vagyon körét, azaz, hogy a Szervezet folyamataiban milyen információk, információhordozók bizalmasságának elvesztése, sérülése, illetve rendelkezésre állása mekkora kárt okoz. Erre alapozható az információs vagyonleltár felvétele. excel file-ban meghatároztuk az információs vagyontárgyak kategóriáit. Ezek:

- HW-eszköz
- Szoftver / Alkalmazás
- Adathordozó
- Papír dokumentum
- Adat/adatbázis
- Infrastruktúra (Helyiségek)
- Infrastruktúra (védelmi rendszerek)
- Kommunikáció
- Személy

Az információs vagyonelemeket a Szervezet működteti, használja, a folyamatok részét képezik, a vagyonelemekhez felelősöket jelöltünk ki. A vagyonelemek felvételekor az excel file-ban rögzítjük:

- A Vagyontárgy megnevezését
- Elhelyezését
- Felelőst

Az információk és adatok hozzáférését személyek egyértelműen meghatározott csoportjára kell korlátozni, és az információkat csak olyan személyeknek szabad kiadni, akiknek azokra egy adott munka kapcsán szüksége van.

Az alkalmazottaknak a személyi adatok kezelését (gyűjtését, feldolgozását és használatát) az igazolt és megengedett célokra kell korlátozniuk.

A személyes adatokat bizalmasan kell kezelni.

Az elektronikus dokumentumokat azok célja és rendeltetése szerint a megfelelő központi dokumentum tároló rendszerben kell elhelyezni. Ezek használatát szükség szerint jogosultság kezeléssel kell szabályozni.

Minden elkészült, kiadott dokumentumból egy példánynak a fenti központi tárolóhelyek egyikén rendelkezésre kell állnia.

El kell kerülni az elektronikus dokumentumok szükségtelen másolatainak elszaporodását, ezért ahol lehetséges ott az eredeti dokumentum másolatának elhelyezése helyett egy arra mutató hivatkozást kell használni.

A mobil eszközökön céges dokumentum csak ideiglenesen tárolandók.

A mobil eszközökön fogadott, létrehozott vagy feldolgozott dokumentumokat a lehető leghamarabb az erre a célra meghatározott központi dokumentum tároló rendszerben kell  a biztonsági osztályuknak megfelelően elhelyezni.

Az asztali munkaállomásokon a dokumentumok kezelését úgy kell végezni, hogy azok csak a feldolgozás idejére legyenek helyben tárolva, a feldolgozást követően az előző pontokban meghatározott központi tároló helyre kerüljenek. Ha a munkavégzéshez közvetlenül már nem szükséges, akkor a helyi másolatot törölni kell.

Minden központi dokumentum-tároló rendszernek lehetővé kell tennie a hozzáférési jogosultságok gyors és egyértelmű kiadását és visszavonását valamint az éppen érvényes jogosultságok könnyű áttekintését.

Az elektronikus üzenetküldő rendszerek (VoIP alkalmazások) nem használandók a dokumentumok tárolására vagy terjesztésére.

**Kockázatértékelés**

Az információs vagyonleltár minden elemére megvizsgáljuk, hogy azok sérülése, elvesztése, megsemmisülése esetén vagy azok hatására egyéb módon, a védendő információ bizalmassága, sértetlensége és/vagy rendelkezésre állásának sérülésén keresztül mekkora kár érheti a Szervezetet.

Az adatkörök és a kárérték meghatározásnál kiemelten vesszük figyelembe ügyfeleink igényeit a szolgáltatás folytonosság és rendelkezésre állás viszonylatában.

A kockázatértékelés operatív módon a fent említett vagyonleltár excel file kiegészítésével történhet. Ehhez a fent említett excel munkalapot további oszlopokkal egészítjük ki:

- Veszélyforrás (Mi történhet)
- Káresemény (Mit okozhat)
- Jelenlegi védelem
- Bekövetkezés valószínűsége
- Kár „C” (Bizalmasság)
- Kár „I” (Sértetlenség)
- Kár „A” (Rendelkezésre állás)
- Kár maximáslis értéke
- Kockázat
- Megjegyzés

A kezelhetőség szempontjából elegendő, ha minden egyes vagyonelemre az elsődleges és legnagyobb hatású Veszélyforrást rögzítjük és az ezzel kapcsolatos Káreseményt figyelembe véve végezzük az értékelést.

Minden vagyonelem és minden hozzá felvett elsődleges veszélyforrás esetén megvizsgáljuk az adott veszélyforrás adott vagyonelem esetén történő bekövetkezési valószínűségét. Itt figyelembe vesszük az adott vagyonelem vonatkozásában a már jelenleg is működő biztonsági intézkedéseket, azok alkalmazási gyakorlatát.

A C-I-A becsült kárnagyságok közül a maximális értéket vesszük figyelembe a kockázati érték számításánál, melyet a Bekövetkezés valószínűsége és a max. Kár értékének szorzatából kapunk.

Ezek alapján összemérhetők az egyes veszélyek, veszélyeztető tényezők egymáshoz mérhető kockázata. A kockázati érték alapján felállított rangsorban a cégvezetésnek meg kell határoznia és jóvá kell hagynia az elfogadható kockázati szintet. Ezt a szintet meghaladó kockázatok esetében (a meglévőhöz) további védelmi intézkedéseket kell meghatározni.

A Megjegyzés mezőben rögzíthetők a védelmi intézkedések vagy az azokra történő hivatkozások.

**Kockázatkezelés**

A védelmi intézkedések kigondolása után mérlegeljük azok bekerülési és üzemeltetési költségeit, majd azokat összevetjük a bevezetés várható hasznával. Csak pozitív mérleg esetén teszünk javaslatot az intézkedés bevezetésére, amelyet utána annak részletes megtervezése, szabályozásának kidolgozása követ. Az intézkedések bevezetésekor fontos annak feltételeit biztosítani, az érintetteket oktatni, majd magát az intézkedést ellenőrzötten bevezetni. (Célszerű több intézkedési alternatívát végig gondolni, és a legelőnyösebb mellett dönteni.)

A Szervezet az információbiztonsági kockázatok csökkentése és kezelése érdekében bevezetett állandó szabályozásokat, kötelezően alkalmazandó eljárásokat az Információbiztonsági Szabályzatban (IBSZ) foglalja össze.

A kockázatértékelési és kezelési folyamatot minimum évente érdemes elvégezni, ezzel biztosítva az információvédelmi intézkedések aktualitását.

**A vagyonelemek felelősei**

A Szervezet különös figyelmet fordít a Tárgyi Eszközökkel való hatékony gazdálkodásra, ezért a felmerülő igényeket ennek szem előtt tartásával igyekszik kielégíteni, és a használaton kívüli eszközöket felhasználni.

A Szervezet nem támogatja az idegen tulajdonban lévő, felhasználási engedély nélküli tárgyi eszközök munkavégzéshez köthető használatát. Ez alól kivételt képeznek a Vezető által egyedi elbírálással engedélyezett eszközök.

A munkavégzéshez szükséges eszközöket a Szervezet szerzi be és a költségeket is maga fizeti meg.

A Megbízott Rendszergazda rendszeresen ellenőrzéseket végez, melyek során vizsgálja a nyilvántartás és az eszközhasználat megfelelőségét, az e Szabályzatban foglaltak betartását és betartatását.

A Szervezet Pénzügyi Vezetője rendszeres időközönként leltárt készít, hogy alátámassza a mérleg valódiságát.

Az informatikai eszközök felhasználók között, illetve a raktárba történő helyezése során gondoskodni kell a felhasználói igények szerinti adatmentésekről, adatmentesítésekről.

Felhasználókra vonatkozó általános szabályok:

- A Felhasználó kötelezettsége azon Tárgyi Eszközökkel való elszámolás, melyek a Felhasználó által leadott és a Szervezet részéről engedélyezett igénynek megfelelően megrendelésre, leszállításra, valamint átvételre kerültek.
- A Szervezet valamennyi Felhasználója Tárgyi Eszközt csak a tulajdonában kezelt folyamatokon keresztül vehet birtokba, adhat át és csak az előzetes jóváhagyásokat követően használhat. Valamennyi Tárgyi Eszköz átadása-átvétele a vonatkozó jogszabályok, valamint jelen Szabályzatban rögzített módon történik.
- A Szervezet valamennyi Felhasználója köteles a Tárgyi Eszköz állapotában (mennyiségében vagy minőségében) bekövetkezett változást a Megbízott Rendszergazdának haladéktalanul jelenteni, és arról a változást megfelelően rögzítő jegyzőkönyvet felvetetni.
- A Tárgyi Eszközökben Felhasználók által okozott károkért (gondatlan, vagy szándékos károkozás) a Felhasználók anyagi felelősséggel tartoznak.
- A Felhasználó a Szervezet által végzett, az eszközgazdálkodási területet érintő ellenőrzések során köteles együttműködni az ellenőrzést végző személyekkel, és minden információt megadni számukra a tárgyi eszközökkel kapcsolatban.
- A jelen szabályzatban előírtaktól való eltérés csak a Vezető engedélye esetén megengedett.
- Amennyiben a Szervezet munkatársnak nincs szüksége az eszköz további használatára, úgy a Felhasználó írásban kezdeményezi a Vezető felé az eszköz átadását.
- A Szervezet Eszköz Kiadási Szabályzatának visszavételi jegyzőkönyv kitöltése után a Vezető meggyőződik:
- A jegyzőkönyven feltűntetett adatok helyességéről
- A visszaszolgáltatott eszköz(ök) állapotáról
- Az eszközt visszaszolgáltató eltávolítja az összes olyan alkalmazást az eszköz formatálásával, amely a birtokba vétel előtt nem volt telepítve az adott eszközön.

**A cserélhető adathordozók kezelése**

Az adathordozók biztonságos kezelésének kialakításával megakadályozható a Szervezet magasabb szintű adatbiztonsági kategóriákba besorolt adatainak illetéktelen kézbe való kerülése. A Szervezet tulajdonában lévő és bérelt, a magasabb szintű adatbiztonsági kategóriákba besorolt adatok tárolására használt adathordozókat, amennyiben az a kockázati értékelésen egy előzetesen meghatározott értéket elér, azt egyedi azonosítóval kell ellátni, nyilvántartást kell vezetni róla. Az adathordozóra tett címkén, az adattal dolgozó Szervezet munkatársat fel kell tüntetnie az adott tartalomra vonatkozó bizalmassági kategóriákat. Kezelését ennek megfelelően kell megvalósítani.

Adathordozók tárolására vonatkozó szabályok:

- figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket, a tároló helynek tűzbiztos, elektromágneses hatásoktól védett helynek kell lennie,
- az adatbiztonsági kategóriákba besorolt adatokat tartalmazó adathordozók tárolásánál figyelembe kell venni a szabályzat adatok kezelésével kapcsolatos előírásaiban megfogalmazottakat,
- két példányban való tárolás esetében a tároló helyet úgy kell kiválasztani, hogy szükség esetén az arra jogosult akadálytalanul és viszonylag gyorsan hozzáférhessen, de célszerűen, viszonylag távol legyen egymástól a két tárolásra szolgáló helyiség (amennyiben ez értelmezhető), ezzel megakadályozva mindkét példány egyidejű megsemmisülését természeti katasztrófa esetén,
- adathordozókat zárható szekrényben kell őrizni/tárolni, amikor éppen nincsenek használatban, főként a munkaidőn kívüli időszakban.
- USB portok és optikai meghajtók írási jogának korlátozása az egyes számítógépeken
- Amennyiben elkerülhetetlen az adatok másolása mobil adattárolóra (CD, DVD, mobil winchester, USB drive, stb.), az adattárolón a tárolást tikosítva kell megvalósítani.

**Adathordozók eltávolítása**

Megsemmisítés/törlés: Csak az Adatgazda (Adatvagyonleltárban megjelölt felelős) engedélyével törölhető/semmisíthető meg. Az elektronikus adathordozón lévő adatokat törölni kell (minőségi törléssel, többszöri felülírással), a hibás adathordozókat fizikailag meg kell semmisíteni.

A Szervezet mindaddig elzárva tárolja a meghibásodott adathordozókat, ameddig azok szakszerű fizikai megsemmisítése és elszállítása meg nem történik.

A maximális élettartamuk lejárta után az adathordozókat át kell másolni új adathordozóra, majd a régi adathordozót le kell selejtezni, és meg kell semmisíteni,

Megsemmisítéskor az adathordozót fizikailag kell megsemmisíteni, és az IBSZ 4. mellékletében szereplő megsemmisítési jegyzőkönyvben szükséges vezetni.

Az adathordozót le kell selejtezni akkor is, ha vélhetően az adathordozó hibája miatt az adatmentés sikertelen volt, illetve ha a katasztrófa vagy visszatöltési próbák során az adat visszatöltés sikertelenné vált.

Amennyiben az adathordozón elérhető még a tartalma, a selejtezés előtt szükséges minőségi törléssel eltávolítani az adathordozón lévő adatokat.

Fizikai adathordozón vállalati információt a Szervezet Irodájából kivinni csak a Vezető Írásos engedélye esetén lehetséges. Minden más esetben fegyelmi eljárást von maga után.

# Üzemeltetési és fejlesztési eljárások

Az üzemeltetési dokumentációért a Megbízott Rendszergazda a felelős. Az üzemeltetési dokumentációnak a rendszerek használatbavételekor rendelkezésre kell állnia. A Megbízott Rendszergazda a felelős az üzemeltetési dokumentáció naprakészen tartásáért.

**Változásfelügyelet**

A változások tervezése és végrehajtásuk dokumentálása ebben a fejezetben leírtak alapján történik. A változáskezelési folyamatot megfeleltetjük az információbiztonság alapvető követelményeinek, ezért biztosítania kell az alábbiakat:

- Az üzemeltetési szabályzatokban történő változások folyamatos dokumentálása.
- A változások, amennyiben ez technikailag lehetséges, előzetes tesztelése, modellezése, tesztadatokkal (nem használható éles adatbázis)
- A változások információbiztonsági hatásainak elemzése a változás megtervezésekor.
- A változáskezelési folyamatba a Vezetőt jóváhagyási joggal be kell vonni.
- A változáskezelési folyamatnak képesnek kell lennie a vezetőség által kezdeményezett sürgős információbiztonsági intézkedéseknek a lehető legkisebb késedelemmel történő végrehajtására.
- A jelentős, vagy különösen kockázatos változások esetén kockázatelemzés elvégzése.
- A változással érintett BCP tervek és a Mentési tervek aktualizálása.
- A változás sikertelenségének esetére a visszaállási terv elkészítése.

**A szoftverfejlesztéssel és üzemeltetéssel kapcsolatos elvárások**

A következő fő információbiztonsági és GDPR által támasztott szempontokat szükséges figyelembe venni a biztonságos szoftverfejlesztés és támogatási folyamatok betartásának érdekében:

- A szoftvernek szükséges megfelelnie a GDPR rendeletben támasztott adatkezelési alapelvek érvényesíthetőségének, különös tekintettel az integritásra és bizalmas jellegre (5. cikk (1) f)).
- Az érintettek jogainak érvényesítési szándéka esetén a rendszer megfelelő felkészítése szükséges, fokozott figyelemmel a törléshez- (17. cikk), a hozzáféréshez- (15. cikk) és az adathordozhatósághoz való jogra (20. cikk) (adathordozhatósági kérelem esetén az érintett adatait lehetőség szerint .XML vagy .CSV formátumban kell átadni).
- A felhasználók munkájának dokumentációkkal történő segítése, a szoftverek funkcionális működésének megismerése érdekében.
- A kiszervezett fejlesztés során a teljes fejlesztési folyamat felügyelete és a kiszervezett rendszerfejlesztési tevékenységek megfigyelése (szerződéses keretek, biztonsági követelmények, elfogadási és átvételi kritériumok meghatározása).
- A rendszerfejlesztési és integrációs tevékenységek számára biztonságos fejlesztési környezet létrehozása és védelme, amelyek lefedik a rendszerfejlesztés teljes életciklusát.
- A szoftverekben tárolt adatokhoz történő munkatársi hozzáférés lehetőség szerinti szűkítése mezőszinten, így biztosítva a bizalmas jellegnek történő megfelelést.
- A személyes adatokat tartalmazó adatbázisok elkülönített tárolása – amennyiben technikailag megoldható –, így biztosítva azok védelmét és kezelhetőségét (pl.: biztonsági mentés)
- A fejlesztés során történő anonimizált-, vagy teljesen véletlenszerű adatokból álló adatbázis használata, éles adatbázis használatának kerülése.
- A fejlesztési, tesztelési és üzemi környezetek fizikális elkülönítése dedikált szervereken (az üzemi rendszertől logikailag elválasztottan).
- Amennyiben a fejlesztőknek szükséges az éles működési környezetbe történő betekintés, ideális azt a Szervezet telephelyén megvalósítani. A betekintést minden esetben felügyelet mellett indokolt végezni - erre lehet megoldás egy azonosítást igénylő, távoli asztali kapcsolat minden egyéb művelet korlátozásával történő felépítése (pl.: az eszköz egyéb területeihez való

hozzáférés). Amennyiben a Szervezet munkatársának nincs lehetősége a munkamenet felügyeletére, úgy a támogatási folyamatról felvétel készíthető.
- Az éles adatbázis kívülről történő elérhetőségének korlátozása (pl.: belső tűzfal alkalmazásával), írási és olvasási jogosultsággal, csak az adott adatbázist használó szoftver rendelkezhet.
- Elfogadási tesztprogramok, valamint hozzájuk kapcsolódó kritériumok létrehozása az új információs rendszerekre, a továbbfejlesztésekre és új verziókra.
- Biztonsági követelmények alkalmazása minden tervezési szinten, minden architektúra rétegben, ezen biztonsági funkciók tesztelése.
- A szoftvercsomagok módosításának elkerülése, illetve a változtatások szigorú felügyelete.
- Az alkalmazások személyes adatokat tartalmazó adatbázisainak biztosítása annak érdekében, hogy az ne tárolódjon harmadik országban (lehetőség szerint a Szervezet saját felügyelete alatt álló eszközök használata ezek tárolására).
- Az adatbázisok és hozzáférések titkosított tárolásáról való gondoskodás.
- A jegykezelő rendszerekben illetve levelező rendszerekben tárolt személyes adatokat tartalmazó jegyek és kérések egy évig őrizhetők meg vagy amíg más okból az adott személyes adatot törölni szükséges.
- A kritikus infrastruktúra elemeket tároló helyiség kulcsát zárható helyen szükséges tárolni és kulcsfelvételi jegyzőkönyv vezetése szükséges.
- A szerverszoba biztonságát minden külső környezeti és illetéktelen behatás ellen védeni szükséges (pl: zárható rack szekrény alkalamazása).
- Amennyiben szükséges éles adatokkal tesztelni az fejlesztési elemeket, azt minden esetben csak a Szervezet alkalmazottja végezheti, a fejlesztő útmutatása vagy a korábbi gyakorlat alapján.
- A központi NAS tároló saját szünetmentes tápegységgel rendelkezik, így pillanatnyi áramkimaradás esetén folytatható a munkavégzés. Tartós áramszünet esetén pedig a rendszer biztonságos leálítást kezdeményez annak érdekében, hogy a GDPR által támasztott sérteelnség megvalósuljon.

**Intézkedések a rosszindulatú szoftverek ellen**

A Szervezet minden munkaállomása rendelkezik anti-vírus szoftverrel, melyet a felhasználó nem tud a Megbízott Rendszergazda és a Vezető írásos engedélye nélkül kikapcsolni vagy a beállításait megváltoztatni.

- A vírusvédelmi rendszert ki kell terjeszteni minden olyan eszközre, amire a vírustámadás értelmezhető.
- A vírusvédelemnek ellenőrzés alatt kell tartania a mobil adathordozókat is.
- Az elektronikus üzenetküldő rendszerekben és azok kliens oldali alkalmazásaiban is működtetni kell a vírusvédelmet.
- A vírusvédelemnek az úgynevezett Spyware és Malware fenyegetések ellen is védelmet kell biztosítania.
- A vírusvédelmi rendszer által használt adatbázisokat rendszeresen, a gyártó biztosította gyakorisággal, de legalább naponta frissíteni kell, és a frissítéseket központilag menedzselt, ellenőrzött módon a rendszerbe tartozó számítógépekre el kell juttatni.
- A rendszernek tájékoztatást kell adnia a frissítések sikerességéről, a vírus észlelésekről valamint a megtett automatikus ellenlépésekről. (A vállalat által használt szoftver rendelkezik központi menedzsment felülettel, amin keresztül minden egyes munkaállomás vírusvédelemmel kapcsolatos információ látható (adatbázis frissítés időpontja, utolsó ellenőrzés…stb.))
- A notebookokat és más mobil eszközöket úgy kell beállítani, hogy a frissítések a Szervezet rendszerén kívül is megtörténjenek kellő gyakorisággal.
- A Szervezet biztosít az alkalmazottak privát eszközeire (mobiltelefon, tablet, stb.) jogtiszta vírusvédelmi szoftverlicenszt, amennyiben az adott alkalmazott számára okvetlenül szükséges a privát eszköz munkaeszközként történő használata. Jóváhagyott anti-vírus szoftver nélkül privát eszközzel a munkavégzést megkezdeni tilos.
- A Szervezet routerein aktív IDS és IPS működik, amely a külső támadások kiszűri és megakadályozza.

A vírusvédelem működési paramétereit központilag, minden érintett eszközre kötelező érvénnyel kell beállítani úgy, hogy az kellő biztonság mellett a munkavégzést ne akadályozza. Jelszóval kell gátolni ezen beállításoknak a felhasználók általi indokolatlan megváltoztatását.

A rendszer monitorozása a Megbízott Rendszergazda feladata. A monitorozás során a rendszer működőképességének ellenőrzésén túlmenően

- figyelni kell a frissítések megtörténtét a szervereken és a felhasználói gépeken,
- a szervereken és a helyi gépeken a frissítési hibákat mielőbb ki kell javítani,
- oda kell figyelni a rendszer ellenőrzése alól kiesett eszközökre, az okot tisztázni kell,
- figyelni kell a nagyszámú vírus észlelésekre és tisztázni kell az okokat.

A Megbízott Rendszergazda feladata és felelőssége nagyszámú vírus észlelése esetén eldönteni, hogy a vírusvédelmi rendszer képes-e a helyzet kezelésére, vagy további intézkedések szükségesek. Utóbbi esetben haladéktalanul értesíteni kell a Vezetőt és a tömeges vírustámadás esetére alkalmazandó az Üzletfolytonossági Tervben meghatározott felelős személyeket a védekezés megkezdése és a további károkozás megelőzése céljából.

A vírusvédelmi rendszer logjait a rendszerben kell gyűjteni, és legalább egy hónapig meg kell őrizni.

**Biztonsági mentések**

A Rendszergazda a következő rendszerben készít biztonsági mentéseket az adatokról:

| Mentendő adatok jegyzéke | | | |
|---|---|---|---|
| Adat típusa | Mentés helye | Mentés gyakorisága | Megőrzési idő |
| Szerver | Winchester | napi | ... |
| PC | Winchester | Valós idejű | ... |

A felhasználók klienseiről nem szükséges mentést készíteni.

A mentésekhez csak a Vezető és a Megbízott Rendszergazda fér hozzá. Igény esetén a Megbízott Rendszergazda gondoskodik a szerver, vagy adatállomány visszatöltéséről, a visszatöltött állományokra a hozzáférések megfelelő beállításáról.

A mentések sikerességét a mentő alkalmazás naplózza, probléma esetén riaszt, mely alapján a Megbízott Rendszergazda feladata a probléma feloldása, dokumentálása.

A munkatársak email fiókjaikban kötelesek gondoskodni az olyan levelek törléséről, amelynek tartalmával, vagy csatolmányával kapcsolatban a Szervezet megőrzési határideje lejárt. Ide tartoznak a szkennelés útján email fiókban tárolt dokumentumok is.

A munkatársak privát fájljainak szerveren történő tárolása tárolása tilos! Amennyiben a Megbízott Rendszergazda tudomást szerez privát anyagok tárolásának tényéről, a felhasználó számára történő jelzés után (esetleg átadva számára egy külső adathordozón), köteles törölni.

**Kamerarendszerrel kapcsolatos követelmények**

A Szervezet telephelyén kamerarendszer üzemel, amelyek élőképet közvetítenke, de elindíthatók felvétel üzemmódban is. A kamerarendszer képeihez a Vezető és a Megbízott Rendszergazda fér hozzá. A munkavégzéshez szükséges felvételeket a munkatársak kikérhetik vezetői engedéllyel, amit a Megbízott Rendszergazda egy titkosított pen drive-on ad át. A feladatok végeztével a pen-drive tartalmát visszaállíthatatlanul kell törölni.

A kamerafelvételek adatkommunikációja egy logikailag elkülönített hálózaton zajlik.

A kamerarendszer képes arra, hogy egy-egy videórészlet törlésre kerüljön, ha egy Érintett a törlési jogával szeretne élni és ezt nem bírálja felül a Szervezet jogos érdeke.

A kameraképek nem tartalmaznak közterületi képet, illetve fix állásban egy adott, ülő munkát végző munkatárs munkavégzését nem figyeli.

A kameraképek megőrzési idejét szükséges betartani, erre vonatkozó részletes állásfoglalást a Szervezet adatvédelmi szabályzata tartalmaz.

**Eseménynaplózás**

A felhasználói tevékenységeket, kivételeket, hibákat és információbiztonsági eseményeket naplózni kell a működő rendszerekben. Az alábbi információkat kell rögzíteni a logokban:

- az esemény forrása
- az esemény azonosítója, vagy egyértelműen azonosítható megnevezése
- az esemény időpontja,
- az esemény helye, ha értelmezhető és azonosítható
- az eseményben érintett rendszerek, szervizek és felhasználók azonosítja,
- az IP címek ha azonosíthatók.

A Megbízott Rendszergazda köteles az általa felügyelt rendszereket, azok műszaki sajátosságainak figyelembevételével ezen követelmények szerint konfigurálni, oly módon, hogy a naplózott adatok késedelem nélkül a központi loggyűjtő szerverre legyenek továbbítva.

A végfelhasználók tevékenysége naplózásra kerül és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak, amelyekről email értesítést kap a Megbízott Rendszergazda és a Vezető. A Megbízott Rendszergazda biztosítja a napló állományok sértetlenségét, folyamatosan gondoskodik a naplók kiértékelésről, a naplózási szabályok betartását technológiai megoldásokkal is kikényszeríti. A megfigyelt tevékenységek közé tartozik, hogy a végfelhasználók milyen dokumentumokat nyomtattak ki.

A Szervezet a kritikus védendő információk változását naplózza, a naplózás szabályait úgy határozza meg, hogy a nyomon követés és a naplók értelmezése azonnal elvégezhető legyen, és a szokásostól eltérő változások esetén riasztás történjen. A naplófájlok 12 hónapig kerülnek megőrzésre, törekedve arra, hogy a munkatársak privát tevékenységei ne kerüljenek naplózásra.

A Szervezet a naplózás szabályozási rendszerében kitér legalább:

- az operációs rendszerek, informatikai hálózat, a szerverek, az alkalmazási rendszerek, adatbázisok, mappastruktúrák, informatikai és hálózati rendszerelemek hozzáférése,
- fájlműveletekkel kapcsolatos események,
- az alkalmazási rendszereiben történő, az ügyfél- és pénzügyi ágazati titok körébe tartozó adatok (beleértve a tranzakciós adatok) változásai,
- az információs és hálózati rendszerelemek beállításai, paraméterezései.

Az üzemeltető szoftverekkel kapcsolatban a következő szempontokat szükséges betartani:

- Biztosítani kell, hogy a szoftverek csak megfelelően képzett szakemberek által kerüljenek telepítésre és megváltoztatásra.
- Biztosítani kell, hogy csak alaposan tesztelt szoftverek, egymással hibátlanul együttműködő szoftver csomagok kerüljenek telepítésre.
- Biztosítani kell, hogy a szoftver ne tartalmazzon fejlesztési kódokat, fordítóprogramokat, hanem csak végleges jóváhagyott végrehajtható kódokat tartalmazzon.
- Biztosítani kell a szoftverekhez a gyártói támogatás rendelkezésre állását. A Megbízott Rendszergazda felelőssége legalább fél évvel a lejárat előtt értesíteni a Szervezetet.

Ezen követelmények teljesítése érdekében:

- A munkaállomáson és mobilszámítógépeken a vállalatnál előírt érvényes szoftvert kell használni.
- A tesztelt, telepíthető szoftvereket a vállalat Ellenőrzött Szoftverkatalógusában kell elhelyezni, és nyilván kell tartani.
- Gyártói támogatással nem rendelkező szoftverek üzletileg kritikus rendszerekben nem üzemeltethetők.
- A gyártói támogatással már nem rendelkező elavult szoftvereket mielőbb le kell cserélni, vagy frissíteni kell.

**Műszaki sebezhetőségek felügyelete**

A műszaki sebezhetőségek ellenőrzés alatt tartása érdekében, a rendszerek műszaki sebezhetőségeit jelentős késedelem nélkül, tervszerűen és ellenőrzött módon ki kell javítani a gyártók által biztosított frissítések, patchek, megkerülő megoldások használatával. Az erről történő gondoskodás a Megbízott Rendszergazda felelőssége és a Megbízott Rendszergazda feladata. A javítások beszerzésére, tesztelésére és telepítésére vonatkozóan az alábbi alapvető követelményeknek kell megfelelni.

- Az IT szolgáltatásokat biztosító kiszolgálókon és hálózati elemeken minden javítás telepítését az üzleti igényekhez igazodva, a lehetséges teljesítmény csökkenés és szolgáltatás kiesés kockázatára figyelemmel csak a rendelkezésre álló javítás megfelelőségének gondos ellenőrzése után, megtervezett módon, ütemezetten szabad és kell végrehajtani, úgy, hogy közben biztosítják a javítás előtti állapotra történő azonnali visszaállás lehetőségét.
- A Windows alapú munkaállomások sebezhetőségeinek javítására központilag felügyelt rendszert kell működtetni, amely a felhasználók beavatkozása nélkül gondoskodik a javítások telepítéséről (Csoportházirend). A javításokat a kiadás előtt alaposan tesztelni kel, hogy nem okoznak-e akadályt a felhasználók munkájában. Ennek érdekében a tesztelést minden a Szervezetnél jellemző felhasználói környezetben (eszközök és alkalmazások) el kell végezni. A javítások kiadása csak jóváhagyás után történhet meg, ezt naplózni kell. Figyelemmel kell kísérni, hogy a javítások kiadása során fellépő hibákat (sikertelen, vagy elmaradt telepítéseket), azokat ki kell javítani. Gondoskodni kell róla, hogy arról, hogy azok a mobil eszközök se maradjanak ki tartósan a javítások telepítéséből, amik hosszabb ideig távol vannak.
- A Unix/Linux alapú rendszerekhez megjelenő javítások figyelemmel követése, beszerzése, ellenőrzése és telepítése a Megbízott Rendszergazda által megjelölt (Unix/Linux Specialista) munkatárs feladata. A javításokat csak abban az esetben kell alkalmazni, ha azok az adott rendszeren futó szolgáltatások szempontjából érintettek.
- A BIOS/ROM/FIRMWARE jellegű frissítéseket csak abban esetben kell telepíteni, ha azok üzleti szempontból lényeges hibák vagy sérülékenységek kijavítását, funkció bővítést eredményeznek.
- A Szervezet által használt számítógépek dedikált UTP portokhoz tartoznak, így külső számítógépek hálózati csatlakoztatása nem lehetséges.
- A Szervezetnél elkülönítésre került egy vendég Wi-Fi hálózat.
- A Szervezet külső szakértő segítségével etikus hackelést folytat le, amelynek eredményeként feltárásra kerülnek a legsúlyosabb biztonsági rések.

Amennyiben olyan sebezhetőség kerül nyilvánosságra, amely súlyosan veszélyezteti az üzemelő rendszerek biztonságát, akkor a Megbízott Rendszergazda sürgősségi javítást rendel el, amit késedelem nélkül végre kell hajtani.

# Az információbiztonsági incidensek kezelése

Minden olyan eseményt, emberi cselekedetet illetve gépi működést információbiztonsági eseménynek tartunk, ami az IBSZ-ben meghatározott alapelvek, célok illetve szabályok megvalósítását, érvényesülését, vagy betartását megsérti vagy közvetlenül fenyegeti függetlenül az elkerülhetetlen véletlen vagy szándéko jellegétől.

Példák információbiztonsági eseményekre:

- Rendelkezésre állás sérülésére utaló események
    - IT eszköz meghibásodása
    - hálózati kapcsolatok megszakadása
- Sértetlenséget veszélyeztető jellemző események
    - vírustámadás
    - adatok megváltozása
- Bizalmasságot veszélyeztető jellemző események
    - illetéktelen hozzáférés
    - hálózati behatolás

**Felelősségek és eljárások**

Az információbiztonsági események kivizsgálása a Megbízott Rendszergazda és az Adatvédelmi Tisztviselő feladata.
A vizsgálat során meg kell állapítani, hogy:

- Milyen események történtek?
- Az események milyen és mekkora kárt okoztak, illetve okozhattak?
- Milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez?
- Mik voltak az események kiváltó okai, előzményei?
- Kik az eseményért közvetlenül és közvetve felelős személyek és milyen a felelősségük mértéke?
- Történt-e bűncselekmény?

A vizsgálatnak gyorsnak és lényegre törőnek kell lennie. Amennyiben visszaélés gyanúja merül fel, az érintett személytől az ügy kivizsgálásának befejezéséig jogosultságait és betekintési engedélyeit vissza kell vonni, az általa ismert jelszavakat meg kell változtatni és más további érdeksérelmet megelőző intézkedéseket kell foganatosítani. Az Adatvédelmi Tisztviselő a kivizsgálás eredményéről írásban is tájékoztatja az ügyvezetést. A tájékoztatásban javaslatot kell tenni a felelősségre vonandó személyekre, illetve a további hasonló károk, biztonságsértések elkerülésére teendő intézkedésekre.

Amennyiben az információbiztonsági esemény a vállalat felelősségi körén belül ügyfél rendszereket, vagy adatokat érintően történik, az Adatvédelmi Tisztviselő kötelessége az ügyfél (vagy vállalati kapcsolattartójának) értesítése, azzal való együttműködés és folyamatos tájékoztatása a vizsgálat során.

**Információbiztonsági események jelentése**

A munkatársak feladatai információbiztonsági események észlelésekor:

- Minden vélt vagy valós információbiztonsági incidenst a Munkatársaknak e-mailben azonnal jelenteni kell az Adatvédelmi Tisztviselőnek, aki az incidenst a megfelelő elektronikus feljegyzésben rögzíti. Alapesetben a belső nyilvántartásban kerül feljegyzésre illetve kockázat felmerülése esetén a NAIH által biztosított felületen is.
- A jelentésben minél pontosabban meg kell adni az esemény leírását és annak körülményeit. Az Adatvédelmi Tisztviselő szükség szerint a Vezetővel közreműködve intézkedik az incidens kezelésére.
- A munkatársak kötelesek az intézkedő személyektől a további teendőkre vonatkozóan kapott utasításokat haladéktalanul végrehajtani.

- A bejelentő munkatársak az eseményről harmadik felet külön felhatalmazás nélkül ne értesítsenek, ne nyilatkozzanak.

Az Adatvédelmi Tisztviselő feladatai az információbiztonsági események bejelentésekor:

- rögzítsen minden a bejelentésben foglalt körülményt és eseményt, a Megbízott Rendszergazdával egyeztetve prioritás szerint kategorizálja a bejelentést;
- szükség esetén a Megbízott Rendszergazda bevonásával tevékenyen kezdeményezze az esemény okozta károk csökkentését, az esemény további kiterjedésének megakadályozását;
- az esemény jellegétől függően a bejelentést késlekedés nélkül továbbítsa/eszkalálja a megoldásra kijelölt személy felé.
- Minden olyan esetben, amikor valamilyen bűncselekményre (például lopás) vagy súlyos hanyagságra (elvesztés), vagy szándékos károkozásra utaló körülmény áll fenn, az Értesítendő Személyek működjenek együtt a bejelentővel a bizonyítékok összegyűjtése és hiteles megőrzése érdekében.
- az esemény lezárásakor küldjön visszajelzést a bejelentőnek, amiben tájékoztatja az esemény mivoltáról, az esemény kezelésének menetéről és eredményéről.

Az Adatvédelmi Tisztviselő a felelős az egyes bejelentések prioritás szerinti kategorizálására, valamint az eszkalációs lépésekre vonatkozóan.

A Megbízott Rendszergazda bejelentési kötelezettsége:

Amennyiben a rendszer üzemeltetők a monitorozó rendszertől kapott riasztások, vagy a rendszerek kezelése karbantartása során tapasztalnak vélhető vagy valós információbiztonsági eseményt, amely a bizalmasság vagy a sértetlenség sérülésére utal, akkor azt késlekedés nélkül ugyanúgy jelentsék a Vezető és az Adatvédelmi Tisztviselő felé. A továbbiakban az Adatvédelmi Tisztviselőtől kapott utasítások szerint járjanak el.

Az adatvédelmi incidenst a Szervezetnek indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az GDPR 55. cikke alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

A Rendelet szigorú eljárási követelményeket tartalmaz az adatvédelmi incidensek bekövetkezése esetére. A Szervezetnek kötelessége haladéktalanul, de legkésőbb az incidens észlelését követő 72 órán belül jelenteni azt a NAIH-nak. Ez alól csak akkor mentesülhet, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ezt a Szervezet csak úgy tudja megállapítani, ha azonnal vizsgálatot végez, amint felvetődik az incidens legenyhébb gyanúja. A vizsgálat során szükséges teljes körűen felderíteni az alábbiakat:

- az incidens körülményei,
- okai,
- pontosan milyen adatokat, mekkora alanyi kört érint,
- mennyiben sérültek az érintettek jogai és szabadságai
- mi vezethetett az incidenshez,
- milyen következményekkel jár,
- mennyiben sérültek az érintettek jogai és szabadságai,
- milyen eszközökkel tudja a Szervezet enyhíteni a következményeket,
- az incidens kezelését követően milyen intézkedéseket kell hoznia, hogy többet ne történhessen ilyen.

A 72 órás határidő minden esetben érvényes, ez alól a szabad-, ünnep- és munkaszüneti napok sem képeznek kivételt. Amennyiben a Szervezet a bejelentési kötelezettségének nem tesz eleget, büntetésre számíthat.

A bejelentés során minden lényeges információt közölni kell a hatósággal, így főként, hogy hogyan történt, kik az érintettek, az adatok mely kategóriáját érinti, milyen következményekkel járhat, továbbá milyen intézkedéseket tett a Szervezet a következmények enyhítése érdekében.

**Információbiztonsági gyengeségek jelentése**

Minden munkatársnak feladata, hogy az IT rendszerekben, szolgáltatásokban található bármely megfigyelt vagy gyanított biztonsági gyengeséget jelezze a Megbízott Rendszergazdának és az Adatvédelmi Tisztviselőnek.

A bejelentés történhet szóban vagy írásban, a névtelen bejelentéseket is ki kell vizsgálni.

A bejelentés jellegétől és kihatásától függően az Adatvédelmi Tisztviselő és a Megbízott Rendszergazda intézkedik a kivizsgálásról, és kezdeményezi a sérülékenység megszüntetését.

Az információbiztonság iránti figyelemfelkeltést szolgáló oktatások során az Adatvédelmi Tisztviselő feladata tudatosítani a munkatársakban, hogy semmilyen körülmények között ne kíséreljék meg a vélt vagy valós gyenge pontok ellenőrzését, bejelentésüket bátran tegyék meg. Az Adatvédelmi Tisztviselő a bejelentés eredményéről adjon pozitív tartalmú visszajelzést a bejelentőknek.

**Információbiztonsági események felmérése és döntéshozatal**

Az információbiztonsági incidenset jellegétől függően az arra specializálódott munkatársnak kötelessége kivizsgálni, amely személyt/személyeket a Megbízott Rendszergazda jelöl ki.

A kijelölt munkatárs nem közölhet információkat az incidenssel kapcsolatosan a vizsgálat lezártáig egy munkatárssal sem, kivéve az Adatvédelmi Tisztviselővel és a Vezetővel konzultálhat az incidenssel kapcsolatosan.

**Válasz az Információbiztonsági incidensekre**

Minden egyes bejelentett információbiztonsági incidens bejelentést a lehető leghamarabb (de legfeljebb 24 órán belül) vissza kell igazolni, illetve a kivizsgálást követően a bejelentő felet az eredményről tájékoztatni kell.

**Tanulás az Információbiztonsági incidensekből**

Az információbiztonsági incidenseket évente legalább egyszer a Vezetőségi átvizsgálás keretében ki kell értékelni az információbiztonsági incidensek fajtái, mennyiségei és hatásai figyelemmel kísérése valamint a kezelésüket szolgáló eljárások javítása érdekében.

Az értékelés során az alábbi kérdésekre kell választ adni:

- Reakció idők
    - Milyen gyorsan történt meg az esemény észlelése, kell-e az észlelési idő csökkentése érdekében műszaki intézkedéseket tenni, például monitorozást bevezetni
    - Mennyi ideig tartott, amíg a jelentés a szükséges jelentési utat bejárta
    - Milyen gyors volt a döntéshozatal az esemény kezelésére
    - Mennyi ideig tartott a meghozott döntések, intézkedések végrehajtása
    - Milyen gyorsan sikerült az egyéb érintetteket értesíteni
- Az eszkaláció megfelelősége
    - Helyesen érvényesítették-e az eszkalációs eljárásokat
    - Sikerült-e az eszkalációs döntésekhez kellő információkat összegyűjteni
    - Szükséges-e az eszkalációs eljárás javítása
- Az esemény kivizsgálásának hatékonysága
    - Az esemény súlyosságának megbecsülése helyes volt-e
    - Az esemény kezelése során az üzleti prioritások érvényesültek-e

    - Az esemény kezelését a legmegfelelőbb személyek, szervezeti egységek végezték-e
- Az érintettek megfelelő értesítése
    - Sikerült-e a megfelelő érintetteket időben értesíteni
    - Kell-e az értesítendők körén, elérési módján változtatni
- Visszajelzések a bejelentőknek
    - A bejelentők időben és megfelelően tájékoztatva lett a bejelentésének eredményéről
    - Sikerült-e a bejelentők motiváltságát növelni, az információbiztonság iránti figyelmet javítani
- Az elkövetők motivációjának felderítése
    - Belső eredetű szándékosságra visszavezethető események esetén van-e kapcsolat a munkahelyi légkör és a cselekmény között
    - A motiváció egyedi vagy több személyt is érinthet
    - A motiváció kialakulásában hibáztatható-e valamely munkahelyi vezető
- Eljárások kidolgozása, javítása
    - Indokolt-e az egyes esemény típusokra a kezelésben segítő új eljárások kidolgozása
    - Indokolt-e egyes az üzletmenet folytonossággal kapcsolatos tervek javítása
    - Szükséges-e az oktatás javítása

**Bizonyítékok összegyűjtése**

Az információbiztonsági események kezelése során úgy kell eljárni, hogy a fellelhető bizonyítékokat hiánytalanul és hitelesen összegyűjtsék egy esetleges későbbi jogi eljárásban történő felhasználás érdekében. Ezzel összefüggésben a sértetlenség és bizalmasság sérülését okozó események után a védekező és helyreállító eljárásokat csak a Vezető engedélyével szabad megkezdeni. Az Adatvédelmi Tisztviselő és a Megbízott Rendszergazda feladata a bizonyítékok összegyűjtésére irányuló tevékenységek irányítása, és az összegyűjtött bizonyítékok tárolása, megőrzése, esetlegesen szakértők bevonása is felmerülhet.

A bizonyítékok hitelesítése és hitelességük megőrzése érdekében minden bizonyíték azonosításáról, és kezelésének minden lépéséről jegyzőkönyvet kell vezetni, amit lehetőleg szakértő tanúkkal kell hitelesíttetni.

A bizonyítékokon történő minden tevékenység (például: kiértékelés, jogi eljárásokban történő bemutatás) esetén az eredeti példányok használatát kerülni kell, megbízható körülmények között készített hiteles (megfelelő szakértőkkel hitelesített) másolatokkal kell dolgozni. A bizonyítékok minden lemásolásáról, a másolatok továbbításáról, átadásáról jegyzőkönyvet kell felvenni.

**Adavédelmi Incidens nyilvántartás**

A Szervezetnek szükséges incidens nyilvántartást vezetni, amely a következő elemeket tartalmazza:

- Incidens sorszáma,
- Incidens leírása,
- Tudomásra jutás időpontja,
- Incidens kockázata,
- Jelenlegi védelem leírása,
- Valószínűsíthető következmények,
- Adatvédelmi tisztviselő neve,
- Adatvédelmi tisztviselő elérhetősége,
- Tájékoztatás időpontja,
- Kapcsolattartó neve (amennyiben adatvédelmi tisztviselővel nem rendelkezik a Szervezet),
- Kapcsolattartó elérhetősége (amennyiben adatvédelmi tisztviselővel nem rendelkezik a Szervezet),

Az incidens bejelentő minta Excel táblát jelen Szabályzat 1. melléklete tartalmazza.

# Adatvédelmi Hatásvizsgálati eljárásrend

Az adatvédelmi hatásvizsgálat célja, biztosítani, hogy a Szervezet elektronikus információs rendszereiben történő fejlesztéseknél a tervezett adatkezelési műveletek a személyes adatokat megfelelően védjék.

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 Szervezet az 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:

- 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;

- a személyes adatok különleges kategóriáira vonatkozó személyes adatok nagy számban történő kezelése; vagy

- nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben a Szervezet által érvényesíteni kívánt jogos érdeket;

- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;

- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és

- 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 Szervezet szükség 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.

A hatásvizsgálatokat nyilvántartó minta Excel táblát jelen Szabályzat 2. melléklete tartalmazza. A hatásvizsgálatok elvégzésére a NAIH által biztosított szoftvert használja a Szervezet, amely a következő linken elérhető: https://www.naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html.

Az adatvédelmi hatásvizsgálat elvégzése az Informatika és az Adatvédelmi Tisztviselő felelőssége.

# A működésfolytonosság biztosításának Információbiztonsági vonatkozásai

Szervezetünk a működés folytonosságot, illetve ennek zavara vagy kiesése esetén a csökkentett működést, majd a teljes funkcionális helyreállítást a BCP tervben szabályozta és ilyen esetben annak megfelelően kell eljárni. A működés helyreállításáért a Vezető és a Megbízott Rendszergazda közösen felel.

Az Információfeldolgozó eszközök rendelkezésre állására, az esetleges tartalékok biztosítására vonatkozó biztonsági intézkedések a BCP részét képezik.

A részletes szabályzat megtalálható a Szervezet Működésfolytonossági szabályzatában.