**Szekszárdi Vagyonkezelő Kft.**

# Adatvédelmi és Adatbiztonsági Szabályzata

Székhely: 7100 Szekszárd, Bezerédj u. 2.

**KÉSZÜLT:** **2012.**

**MÓDOSÍTVA:** **2018.**

**2020.**

Bálint Zoltán

ügyvezető igazgató

## Tartalom

## Preambulum

A parkolók üzemeltetése terén a parkolási díjak és pótdíjak beszedése, az önkormányzati tulajdonú ingatlan bérlőivel és a piaci árusító helyek bérlőivel a kapcsolattartáshoz a szükséges adatok nyilvántartása és számlázása, a gyermekek táboroztatásával kapcsolatos adatrögzítési feladatok végzése, valamint a szükséges iratok és adatok feldolgozása megköveteli az adatvédelemmel, a személyes adatok védelmével kapcsolatos feladatok egységes rendszerbe foglalását.

A szabályozás biztosítja az adatvédelmet, és szabályozási garanciákat teremt, amelyek alapján az adatvédelem a lehetőségekhez képest a legmagasabb szinten valósítható meg. Az adatvédelem területén megfogalmazott intézkedések az adatok bizalmasságát, hitelességét és sértetlenségét biztosítják.

A megbízható működés érdekében az informatikai rendszer hardware és szoftver eszközeinek rendelkezésre állását és funkcionalitását biztosító intézkedéseket fogalmaz meg.

**A szabályzat jogszabályi alapjai** a **2011. évi CXII**. törvény az információs önrendelkezési jogról és az információszabadságról szóló (röviden: adatvédelmi) törvény, a társadalmi indokoltság, a személyes részvétel, az érintettek és az adatfajták korlátozása, a célhoz kötöttség, a továbbadás korlátozása, az adathelyesség, az időbeli korlátozás, a nyíltság, a biztonsági intézkedések és a felelősség elveiről és szabályozásáról szóló európai Adatvédelmi törvény rendelkezései, az Európai Parlament által elfogadott „A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről”.
A munka törvénykönyvéről szóló **2012. évi I.** törvény (továbbiakban Mt.) a személyhez fűződő jogokra ( 9.§, 10.§ és a 11.§) vonatkozó előírásai, valamint a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló **2009. évi CXXII**. törvényben és a gazdasági társaságokról szóló **2006. évi IV.** törvényben (a továbbiakban Gt.) megfogalmazottak.

A személyes adatok védelme érdekében - a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 1996-ban adta ki 12. számú ajánlásában meghatározott elvárásoknak is megfelelő - feladatok kerülnek megfogalmazásra, azért, hogy érvényesüljenek az adatok kezelésével, feldolgozásával kapcsolatos különböző jogszabályok előírásai is. **Adatvédelmi szempontból az EU Parlament 2016. május 16-án hatályba lépett adatvédelmi rendelet 2. szakasz 32. cikk adatbiztonsági követelményeinek kell megfelelni**, a **nagy tömegű személyes adatok**, az adatkezelésre használt rendszer bizalmas jellegének, integritásának, elérhetőségének és rugalmasságának biztosítása, a fizikai vagy műszaki probléma esetén a visszaállíthatóság, rendelkezésre állás és hozzáférés biztosítása céljából.

# I. Fejezet

## Az adatok kezelésével összefüggő védelmi szabályok

Jelen Adatvédelmi Szabályzat (továbbiakban: Szabályzat) az adatvédelmi törvényre figyelemmel, és a Vagyonkezelő Kft. biztonságpolitikai elveire épülve készült.

A szabályozás - védelem – célja, hogy az Adatkezelő által kezelt személyes adatok biztonságának kialakítása érdekében meghatározza, és egységes keretbe foglalja azokat az eljárási követelményeket, amelyeket az Adatkezelő valamennyi alkalmazottjának - a rávonatkozó mértékben - ismernie és a biztonsági követelmények érvényesítése érdekében alkalmaznia kell.

Biztosítani a rendkívüli eseményekre, katasztrófa elhárításra, valamint a rendkívüli időszaki kötelezettségekre történő adatvédelmi felkészülést, illetve bekövetkezésük esetén az Adatkezelő adatvédelmi működőképességét.

### 1. A SZABÁLYZAT HATÁLYA, ÉRVÉNYESÍTÉSE:

1.1. A Szabályzat **területi hatálya**:

Kiterjed az Adatkezelő teljes működési területére, valamennyi alkalmazott informatikai eszközre és szoftverre.

1.2. A Szabályzat **személyi hatálya**:

Kiterjed az Adatkezelővel munkaviszonyban vagy munkavégzésre irányuló jogviszonyban álló valamennyi természetes és jogi személyre.

1.3. A Szabályzat **időbeli hatály**a:

A kiadás napjától visszavonásig érvényes.

1.4. Az Adatvédelmi Szabályzat **érvényesítés**e és a megismerési kötelezettség:

Az Adatvédelmi Szabályzat kidolgozása, elkészítése és szükség szerinti módosítása a biztonságért felelős ügyvezető feladata.
A Szabályzatban előírtak betartatásáért hatás- és jogosultsági körére vonatkozóan minden érintett alkalmazott felelős.
A Szabályzatban előírtak betartásának ellenőrzése az ügyvezető feladata.
A Szabályzat előírásait az Adatkezelőnél dolgozó minden személy a szakmai feladatköréhez szükséges mértékben köteles megismerni, a vonatkozó előírásokat betartani és betartatni.
A Szabályzat egyes előírásait, a munkavégzéséhez szükséges mértékben, minden, az Adatkezelővel munkaviszonyban, illetve egyéb szerződéses jogviszonyban álló foglalkoztatottal ismertetni kell.

A Szabályzat előírásait megszegőkkel, illetve a jelentési kötelezettséget elmulasztókkal szemben, a hatályos törvényeknek, rendeleteknek és belső szabályzóknak megfelelő, jogszerű felelősségre vonást kell alkalmazni.

## 2. ÉRTELMEZŐ RENDELKEZÉSEK:

A **személyes adatok köré**be minden olyan adat beletartozik, ami tetszőleges élő személlyel, az érintettel kapcsolatos bármilyen információt hordoz, függetlenül attól, hogy az érintett ezeket mennyire kívánja védeni. Személyes adat az érintettre vonatkozó vélemény, minősítés, továbbá az adatból levonható következtetés is, sőt azok az adatok is személyes adatnak minősülnek, amelyek önmagukban nem, de más személyes adatokkal összekapcsolva az érintettel kapcsolatba hozhatók.
Az adatvédelmi törvény abból indul ki, hogy a személyes adataival mindenki maga rendelkezik, vagyis információs önrendelkezési jogot deklarál, de nem hagyja figyelmen kívül azt sem, hogy e jog nem korlátlan, így lehetővé kell tenni és teszi is a törvény, hogy a személyes adatok kezelését jogszabály elrendelhesse, vagy személyes adatok átadását – bizonyos keretek között –megengedje. A személyes adatok az érintett hozzájárulása nélküli kezelésének, és ehhez átadásának, átvételének igénye elsősorban az államigazgatás, a bűnüldözés területein merül fel, azonban nem hagyható figyelmen kívül az, hogy ez az igény mások jogainak biztosítása érdekében vagy például a gazdasági élet egyes területein is indokolt lehet.

**Adatkezelés**:

Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárult, vagy azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete elrendeli. Az adat kezelésének jogalapja igazolt, célhoz kötöttsége fennáll.

**Adatfeldolgozó:**

Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelő, azaz az adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel.
Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.

**Adatvédelmi incidens:**
A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

**Adatvédelmi kockázatok:**

- adatok feletti rendelkezés elvesztése,
- adatlopás,
- pénzügyi veszteség,
- jó hírnév csorbulása.

## 3. AZ ADATKEZELŐ ÁLTAL VÉGZETT ADATKEZELŐI ÉS ADATFELDOLGOZÓI TEVÉKENYSÉGRE VONATKOZÓ SZABÁLYOK:

### 3.1. Adatfelvétel, adatátvétel, adatigénylés

- Közvetlenül az érintettől felvett adatok.
- Adatfeldolgozóként az adatkezelőtől, mint megbízótól átvett adatok.
- Adatigénylés, közvetlen lekérdezés parkolási díjak és pótdíjak beszedéséhez:

  Az Adatkezelő a BM Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság Közlekedésigazgatási és Nyilvántartási Főosztálya (továbbiakban: BM KNYO) határozata alapján az EPC Hungary Kft.-vel (adatfeldolgozó) megkötött együttműködési megállapodásban és annak szerves részét képező kommunikációs felület leírásában rögzített módon igényelhet adatot a Közúti közlekedési nyilvántartásból.

  Közvetlen lekérdezéseket az Adatkezelő csak az általa szerződéses megállapodásban rögzítettek szerint, az adatfeldolgozó és a BM KNYO Üzemeltetési Főosztálya között kiépített, biztonsági szempontok alapján auditált és felügyelt flexcom vonalon lehet végrehajtani.

  A lekérdezések végrehajtása céljából csak az adatfeldolgozónál erre megnevezett személyek csatlakozhatnak, akik azonosítóval és jelszóval rendelkeznek.

### 3.2. Adatok tárolása

A személyes adatokat a célhoz-kötöttség fennállásáig lehet csak tárolni.

Adatfeldolgozással, adatkezeléssel és az adattovábbítással kapcsolatos technikai adatok tárolása
Az alábbi un. technikai adatokat kell - a tárolt személyes adatok célhoz-kötöttségének megszűnését és törlését követően is - számítógépes nyilvántartásba vett adathordozón 5 évig tárolni:

- Adatigénylés érkezésének dátuma,
- Adatigénylés küldője, csoportazonosítója,
- Személyes adatok lekérdezésének dátuma,
- Személyes adatok felhasználásának módja,
- Személyes adatok továbbításának dátuma,
- Személyes adatok törlésének dátuma

### 3.3. Az adatkezeléssel szemben támasztott követelmények:

- felvételük és kezelésük tisztességes és törvényes;
- pontosak, teljesek és időszerűek;
- tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

### 3.4. Az adatok felhasználása

Személyes adatokat csak a vonatkozó jogszabályokban és engedélyekben megfogalmazott célra lehet felhasználni. Harmadik személynek csak az érintett írásos beleegyezése esetén lehet továbbítani, illetéktelennek átadni tilos.

Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

### 3.5. Tájékoztatás hírközlő eszközön

Hírközlő eszközökön csak olyan tájékoztatás adható, amely a személyes adatok védelméhez fűződő, és az Adatkezelő üzleti és működési érdekeit, valamint az adatvédelmet és adatbiztonságot nem sérti. Felvilágosítás adható általában az Adatkezelő adatkezelői, és az adatfeldolgozó szolgáltatói tevékenységéről, partnereiről, engedélyező és felügyeletet ellátó szervezetekről.

### 3.6. Adatok törlése, helyesbítése

A személyes adatot törölni kell, ha

a) kezelése jogellenes;
b) az érintett kéri;
kivéve, a törvényi felhatalmazás alapján kezelt adatok, ill. jogérvényesítéshez szükséges adatok;
c) az adatkezelés célja megszűnt.

A törlési kötelezettség – a jogellenes adatkezelés kivételével - nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

A törlés tényéről a számítógépes adatbázisban technikai adatként öt évig tárolásra kerül a csoportazonosító és a dátum.

A valóságnak meg nem felelő adatot az adatkezelő, helyesbíteni köteles.

A helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

### 3.7. Adattovábbítás

Az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

Személyes adat az országból - az adathordozótól vagy az adatátvitel módjától függetlenül - külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve, hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek.

### 3.8. Adattovábbítás nyilvántartása

Az adatok átadását, minden esetben, jegyzőkönyvben kell rögzíteni, a jegyzőkönyveket nyilvántartásba vett iktatókönyvbe be kell iktatni. A jegyzőkönyvek elektronikus, napló fájlait is öt évig meg kell őrizni.

Adatátadás céljára csak nyilvántartásba vett elektronikus adathordozó használható. E-mail mellékletként személyes adatokat csak a megbízási szerződések mellékletében rögzített formában, tömörítve és titkosítva lehet továbbítani.

## 4. HATÁSVIZSGÁLAT, MÉRLEGELÉSI TESZT, KOCKÁZAT ELEMZÉSE:

**4.1.** A Rendelet meghatároz néhány körülményt (35. cikk (7) bekezdés), amikor adatvédelmi hatásvizsgálatot kell elvégezni. Ezek a következők:

- 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 kategóriái (Rendelet 9. cikk), vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok (Rendelet 10. cikk) nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

**4.2.** A hatásvizsgálatnak ki kell terjednie:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére (beleértve adott esetben az adatkezelő 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.

## 5. AZ ADATKEZELŐ KÖTELES E TEVÉKENYSÉGE MEGKEZDÉSE ELŐTT AZ ADATKEZELÉST NYILVÁNTARTÁSBA VENNI:

a) az adatkezelés célját;
b) az adatok fajtáját és kezelésük jogalapját;
c) az érintettek körét;
d) az adatok forrását;
e) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját;
f) az egyes adatfajták törlési határidejét;
g) az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;
h) a belső adatvédelmi felelős nevét és elérhetőségi adatait.

Az adatkezelői és adatfeldolgozói tevékenységet, ill. a változásokat nyilvántartásba vétele céljából a NAIH-nál be kell jelenteni.

Az adatkezelőnek a NAIH nyilvántartásba vételkor az alábbi nyilvántartási számokat kapta:

Parkolási díjak és pótdíjak beszedéséhez: **NAIH-58815/2012**
Árusító helyek bérlői azonosító adatainak nyilvántartása: **NAIH-59004/2012**
Lakás és helyiségbérlők személyazonosító adatainak nyilvántartása: **NAIH-61645/2013**
A vásárok és piacok tartásáról szóló rendeletben foglaltak végrehajtása, a piac területének rendészeti ellenőrzése céljából kép és videófelvétel rögzítése: **NAIH-80844/2014**

A nyilvántartási számot az adatok minden továbbításánál, nyilvánosságra hozásánál és az érintettnek való kiadásakor fel kell tüntetni.

Az adatkezelői tevékenységre vonatkozó adatok megváltozását a belső adatkezelési nyilvántartásban módosítani kell.

.

## 6. A KEZELT ADATOK CÉLJA ÉS FAJTÁI:

### 6.1. Személyügyi adatkezelések a munkaviszony létesítése, teljesítése vagy megszüntetése céljából a munkavállaló

- neve,
- születési neve,
- születési helye,
- születési ideje,
- anyja születési neve,
- állandó bejelentett lakcíme,
- tartózkodási hely (amennyiben eltérő a lakóhelytől),
- adóazonosító jele,
- társadalombiztosítási azonosító jele (TAJ-szám),
- nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
- személyazonosító okmány száma,
- lakcímet igazoló hatósági igazolvány száma,
- banki folyószámla száma,
- végzettséget igazoló okmány másolati példánya,
- fénykép.

### 6.2. A meg nem fizetett parkolási díjak és pótdíjak beszedéséhez

- gépjármű forgalmi jele és gyártmánya
- parkolás dátuma és helye
- üzembentartó/tulajdonos családi név és utónév
- üzembentartó/tulajdonos születési ideje és helye
- üzembentartó/tulajdonos anyja neve
- üzembentartó/tulajdonos bejelentett lakcíme/tartózkodási helye
- üzembentartó/tulajdonos hátraléka összege
- adatfeldolgozó, EPC HUNGARY Kft.- nek való átadás dátuma

### 6.3. Árusító helyek bérlői személyazonosító adatainak nyilvántartása

- bérlő neve,
- születési neve,
- születési helye,
- születési ideje,
- anyja születési neve,

- állandó bejelentett lakcíme/tartózkodási hely,
- adóazonosító jele,
- személyazonosító okmány száma,

**6.4. Lakás és helyiségbérlők személyazonosító adatainak nyilvántartása**

- bérlő neve,
- születési neve,
- születési helye,
- születési ideje,
- anyja születési neve,
- állandó bejelentett lakcíme/tartózkodási hely,
- adóazonosító jele,
- személyazonosító okmány száma.

**6.5. Vagyonvédelemmel és kamerás megfigyelő rendszer működtetésével kapcsolatos adatkezelés a** Piac tér 1. Hrsz:1822/2; A és F épület területén, a Szekszárd, Garay tér 19. sz. alatti „Garay Élménypince" helyiségben, valamint a Szekszárd, Széchenyi u. 18-20. szám alatti mélygarázsban.

6.5.1. A kamerarendszer a következő feltételek együttes fennállása esetén üzemeltethető:

- a kamerarendszer kizárólag az emberi élet, a testi épség, a személyi szabadság védelmét, a jogsértő cselekmények megelőzését és bizonyítását, valamint a közös tulajdonban álló vagyon védelmét szolgálja,
- a fennálló körülmények valószínűsítik, hogy a jogvédelem más módszerrel, mint a felvételek felhasználása, nem érhető el,
- alkalmazása a meghatározott célok eléréséhez elengedhetetlenül szükséges mértékig terjed, és nem jár az információs önrendelkezési jog aránytalan korlátozásával.

6.5.2. Kezelő személyek létszáma 3 fő, a Szekszárdi Vagyonkezelő Kft. alkalmazottjai.

6.5.3. képek, videó-felvételek tárolására digitális, beépített merevlemez áll rendelkezésre, amely 30 nap anyagát tudja tárolni.

6.5.4. A piac területén, az „A" épületben 8 db, az „F" épületben szintén 8 db kamera képes az adatokat, képeket továbbítani a központi egységbe.

6.5.5. A kamera-rendszer 0-24 óra működési vagy üzemelési idő/időszakot biztosít és szoftveres mozgásérzékelésre indul a rögzítés.

6.5.6. A kamerarendszer a felvételeket automatikusan rögzíti és a rögzítést követő 3 napig kell tárolni abból a célból, hogy azok a rögzítés helyszínén elkövetett bűncselekmény vagy szabálysértés miatt indult büntető-, szabálysértési vagy más hatósági, bírósági eljárásban - ideértve az érintett személy vagy a társasházi közösség által, jogainak érvényesítése céljából indított eljárásokat, akár a polgári peres eljárást is - bizonyítékként, az erre törvényben felhatalmazott adatkezelők által felhasználhatóak legyenek. E határidő lejártát követően a fel nem használt felvételeket haladéktalanul törölni kell úgy, hogy azok többé ne legyenek helyreállíthatók,

6.5.7. A kamerarendszer nem irányulhat a külön tulajdonban álló lakás vagy nem lakás céljára szolgáló helyiség bejáratára vagy más nyílászárójára,

6.5.8. A kamerarendszer által rögzített felvételekhez kizárólag a rendszer üzemeltetője férhet hozzá, azokat csak a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen esetben jogosult megismerni, és a felvételeket csak a bíróság, a szabálysértési vagy más hatóság részére továbbíthatja,

6.5.9. Az, akinek jogát vagy jogos érdekét a kamerarendszer által rögzített felvétel érinti, a felvétel rögzítésétől számított tizenöt napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak üzemeltetője ne semmisítse meg, illetve ne törölje,

6.5.10. kamerarendszerrel felszerelt épületbe, épületrészbe és a kamerák által megfigyelt területre belépni, ott tartózkodni szándékozó személyek figyelmét jól látható helyen, jól olvashatóan, a megfelelő tájékoztatásra alkalmas módon fel kell hívni az elektronikus megfigyelőrendszer alkalmazásának tényére. A tájékoztatásban meg kell jelölni az üzemeltető személyét és elérhetőségét is. Az üzemeltető az érintett személyt - kérésére - köteles tájékoztatni a felvételek készítésével kapcsolatos minden tényről, így különösen annak céljáról és jogalapjáról, az üzemeltetésre jogosult személyéről, a felvételek készítésének időpontjáról és tárolásának időtartamáról, továbbá arról, hogy kik ismerhetik meg a felvételeket. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira, valamint jogorvoslati lehetőségeire,

6.5.11. az adatkezelés jogalapja a 2005. évi CXXIII. törvény 31. § (1)(2) bekezdése, az Szvtv 30 § (2) bekezdése, valamint az Szvtv 31 § (6) bekezdése,

6.5.12. az adattárolás határideje: 3 nap.

## 7. ADATFELDOLGOZÓI SZERZŐDÉS ALAPJÁN TÖRTÉNŐ ADATKEZELÉS

**7.1.** A Szekszárdi Ipari Park Kft. részére szerződés alapján adminisztrációs szolgáltatás nyújtása keretében ki és bejövő postai küldemények feldolgozása és iktatása,

**7.2.** bérleti szerződések készítése, aktualizálása, személyes adatok kezelése,

**7.3.** követelés kezelése.

## 8. AZ ÉRINTETT JOGAI

**8.1.**Hozzáférési jog, az adatkezelés céljának, a személyes adatok kategóriáinak, tárolásának időtartamának megismerése. Tájékoztatást és másolatot kérhet.

**8.2.**Helyesbítéshez való jog, kérheti a hiányos adatok kiegészítését, helyesbítését.

**8.3.**Törléshez való jog („az elfeledtetéshez való jog”), megszűnik a jogalapja az adatkezelésnek.

**8.4.**Adatkezelés korlátozásához való jog, ha vitatja az adatok pontosságát, ha az adatkezelés jogellenes és ellenzi a törlését, egyben kéri a felhasználás korlátozását.

**8.5.**Az adatkezelés korlátozásához való jog

**8.6.**Az adathordozhatóságához való jog, ha az adatkezelés hozzájáruláson vagy szerződésen alapul, a rá vonatkozó adatokat megkapja, kérheti adatkezelők közötti közvetlen továbbítását.

**8.7.**A tiltakozáshoz való jog, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen.

**8.8.**a jog gyakorlásának biztosítása

**8.9.**Az érintett kérelmére az Adatkezelő tájékoztatást ad az általa kezelt, illetőleg az általa feldolgozott adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat.

**8.10.** Az Adatkezelő köteles az írásos kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a tájékoztatást.

**8.11.** Megtagadás esetén az Adatkezelő köteles az érintettel a felvilágosítás megtagadásának indokát közölni.

**8.12.** Az elutasított kérelmekről az Adatkezelő a nyilvántartást vezet.

## 9. KÖZÉRDEKŰ ADAT ÉS KÖZÉRDEKBŐL NYILVÁNOS ADAT:

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat. A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait - ha törvény kivételt nem tesz - az adatkezeléshez fűződő más érdekek, ideértve a közérdekű adatok nyilvánosságát is, nem sérthetik.

Az Adatkezelő hozzáférhetővé teszi a tevékenységével kapcsolatos legfontosabb - így különösen az illetékességükre, szervezeti felépítésükre, a birtokukban lévő adatfajtákra és a működésükről szóló jogszabályokra vonatkozó - adatokat. A hatáskörében eljáró személyek, ügyvezetők neve és beosztása bárki számára hozzáférhető, nyilvános adat.

Gondoskodni kell, hogy az Adatkezelő kezelésékben lévő közérdekű adatot bárki megismerhesse, kivéve, ha az adatot törvény alapján az arra jogosult szerv állam- vagy szolgálati titokká nyilvánította, illetve ha azt nemzetközi szerződésből eredő kötelezettség alapján minősített adat.

## 10. AZ ADATVÉDELMI FELELŐS, ADATVÉDELMI TISZTVISELŐ:

**10.1.** közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

**10.2.** ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

**10.3.** kivizsgálja a hozzá érkezett bejelentéseket, és a jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

**10.4.** elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;

**10.5.** vezeti a belső adatvédelmi nyilvántartást;

**10.6.** gondoskodik az adatvédelmi ismeretek oktatásáról.

**10.7. Az adatvédelmi tisztviselő jogállása**:

- Az adatvédelmi tisztviselő tevékenységének aktív támogatása a felső vezetés részéről (például igazgatósági szinten).
- Az adatvédelmi tisztviselő részére elegendő idő biztosítása a feladatai ellátására. Ez különösen fontos abban az esetben, ha részmunkaidős belső adatvédelmi tisztviselőt jelölnek ki, vagy ha a külső adatvédelmi tisztviselő az adatvédelmi tevékenységet más feladatok mellett végzi.
- Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában, és elősegíti a GDPR alapvető, például az adatok kezelésére vonatkozó elvekre, az érintett jogaira, a beépített és alapértelmezett adatvédelemre, az adatkezelési tevékenységek nyilvántartására, az adatkezelés biztonságára, valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra vonatkozó rendelkezéseinek végrehajtását.

Megbízási szerződés alapján Euro-Inford Iroda Kft. (székhely: 2151 Fót, Kosztolányi D. u. 11-13.) Cégjegyzékszám: 13-09-185809, Tel./fax: 06 (70) 4217663.
ügyvezető: Szeifert Péter
e-mail cím: dpo@euroinford.hu

## 11. AZ IGÉNYBE VETT ADATFELDOLGOZÓ ÉS TEVÉKENYSÉG:

EPC Hungary Kft. (székhely: 1094 Budapest, Tűzoltó u. 57.).

Az adatfeldolgozó és a BM KNYO között kiépített közvetlen számítógépes vonalon a Megbízó részére a közhiteles nyilvántartásból legyűjti a parkolási díjjal, pótdíjjal tartozó járművek üzembentartójának (tulajdonosának) személyazonosító adatait (név, lakcím, születési idő, anyja neve) és a lekérdezés adataival együtt elektronikus úton átadja az Adatkezelőnek.

## 12. ADATVÉDELMI SZABÁLYOK MEGSÉRTÉSÉNEK ESTEI:

**12.1.** A szabályozás megsértéséből származó jogosulatlan és/vagy célhozkötöttség nélküli adatkezelés, adattovábbítás vagy adatátadás,

**12.2.** Hanyag vagy gondatlan magatartással ok-okozati összefüggésbe hozható illetéktelen hozzáférés személyes adatokhoz,

**12.3.** Az adat- és informatikabiztonsági szabályzatban foglaltak (rezsimszabályok) be nem tartása miatt bekövetkezett adatvesztés, adatsérülés,

**12.4.** Jogosulatlan vagy a céltól eltérő adatkezelés,

Adatkezelésnek tekintendő a személyes adatok felvétele, tárolása, feldolgozása, hasznosítása, megváltoztatása és a további felhasználásának a megakadályozása. Az adatkezelés akkor jogszerű, ha ahhoz az érintett hozz ájárul, illetve ennek hiányában is, ha az adatkezelést törvény vagy törvényi felhatalmazás alapján helyi önkormányzati rendelet írja elő. Személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet kezelni. Ez esetben is csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas és csak a cél megvalósulásához szükséges mértékben és ideig. Ami e körbe nem illeszthető, az már az adatkezelés célhoz kötöttsége szabálya megsértésének minősül.

**12.5.** Tájékoztatási kötelezettség megszegése,

Az érintett kérelmére az adatkezelő köteles tájékoztatás adni az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. Az adattovábbításra vonatkozó nyilvántartás és ennek alapján a tájékoztatási kötelezettség időtartamát az adatkezelést szabályozó jogszabály korlátozhatja. A korlátozás időtartama személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb nem lehet. Az érintett tájékoztatása csak honvédelemi, nemzetbiztonsági, bűnmegelőzési és bűnüldözési érdekből tagadható meg. Az érintett polgári per útján (keresettel) érvényesítheti a tájékoztatáshoz fűződő jogát, míg a tájékoztatási kötelezettségét nem teljesítő, az adatot eltitkoló adatkezelő magatartása bűncselekménynek minősül.

## 13. ADATVÉDELMI INCIDENS JELENTÉSE:

**13.1.** Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az GDPR 55. cikk alapján illetékes felügyeleti hatóságnak, NAIH-nak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

Közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

Ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

**13.2.** Az adatvédelmi incidensek nyilvántartása:

- az adatvédelmi incidenshez kapcsolódó tények,
- annak hatásai,
- tett intézkedéseket.

**13.3.** Az érintett tájékoztatása az adatvédelmi incidensről:

- Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
- Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az intézkedéseket is.
- Az érintettet nem kell tájékoztatni, ha az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.
- Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását.

**13.4.** Adatbiztonsági intézkedés elmulasztása

Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

**13.5. Szankciók (a magatartás által bekövetkezett sérelem, érdeksérelem súlyától függően):**

Vezetői figyelmeztetés,

Fegyelmi eljárás,

Büntető feljelentés.

## 14. VAGYONVÉDELMI KAMERA RENDSZER ALKALMAZÁSA:

A 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban Vvtv.) 26. § (1) pontja alapján az Adatkezelő jogosult a területén (magánterület) elektronikus megfigyelőrendszert kiépíteni.

A Vvtv. 28. (2) pontja alapján a közönség számára nyilvános magánterületen jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon köteles figyelemfelhívó jelzést, ismertetést elhelyezni.

A Vvtv. 31. (2) pontja alapján a rögzített kép-, hang-, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított három munkanap elteltével meg kell semmisíteni, illetve törölni kell.

A felvételek megtekintésére az Ügyvezető és az Adatvédelmi felelős jogosult.

## 15. TÁRGYALÁSON KÉSZÜLT HANGFELVÉTEL

Tárgyalásokkor a későbbi írásos jegyzőkönyv készítése érdekében hangfelvétel készülhet. A rögzítés lehetősége hozzájáruláson alapul, így az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 20. § (2) pontja alapján a felvétel megkezdése előtt az érintetteket egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

A hangfelvétel csak saját felhasználásra készíthető, azt másik fél számára nem adható ki. A hangfelvételt az írásos jegyzőkönyv elkészítése után 1 munkanappal, de legkésőbb a hangfelvétel készítése után 10 munkanappal később meg kell semmisíteni.

# II. Fejezet

# Általános szabályok

Jelen Számítástechnikai Védelmi Szabályzat (továbbiakban: Szabályzat) az adatvédelmi törvényre figyelemmel, és a Szekszárdi Vagyonkezelő Kft. biztonságpolitikai elveire épülve készült.

## 16. A SZABÁLYOZÁS - VÉDELEM - CÉLJA:

1.1. A Szekszárdi Vagyonkezelő Kft. üzletpolitikája és üzletmenete biztonságának kialakítása érdekében meghatározni, és egységes keretbe foglalni azokat a biztonsági hardware és software feltételeket, valamint informatikai rendszeralkalmazási- és eljárási követelményeket, amelyeket a Szekszárdi Vagyonkezelő Kft. valamennyi alkalmazottjának - a rávonatkozó mértékben - ismernie és a biztonsági követelmények érvényesítése érdekében alkalmaznia kell.

1.2. Biztosítani a rendkívüli eseményekre, katasztrófa elhárításra, valamint a rendkívüli időszaki kötelezettségekre történő informatikai felkészülést, illetve bekövetkezésük esetén a Szekszárdi Vagyonkezelő Kft. informatikai működőképességét.

## 15. A SZABÁLYZAT HATÁLYA

2.1. A szabályzat **területi** hatálya:

Kiterjed a Szekszárdi Vagyonkezelő Kft. teljes működési területére, valamennyi alkalmazott informatikai eszközre és szoftverre.

2.2. A szabályzat **személyi** hatálya:

Kiterjed a Szekszárdi Vagyonkezelő Kft.-vel munkaviszonyban vagy munkavégzésre irányuló jogviszonyban álló valamennyi természetes és jogi személyre.

2.3. A szabályzat **időbeli** hatálya: a kiadás napjától a visszavonásig érvényes.

## 16. A SZABÁLYZATBAN FOGLALTAK ÉRVÉNYESÜLÉSÉHEZ SZÜKSÉGES FELTÉTELRENDSZER:

3.1. A Szekszárdi Vagyonkezelő Kft. informatikai és informatikavédelmi eszközei működtetéséhez szükséges pénzügyi fedezetet folyamatosan biztosítani kell.

3.2. Az informatikai védelmi tevékenység ellátásához kapcsolódó személyi és tárgyi feltételeket, a prioritásoknak és a Szekszárdi Vagyonkezelő Kft. esetleges szervezeti változásainak megfelelőn kell érvényesíteni.

## 17. A SZABÁLYZAT ÉRVÉNYESÍTÉSE:

A védelmi szabályzat kidolgozása, elkészítése és szükség szerinti módosítása a biztonságért felelős személy feladata;

- a szabályzatban előírtak betartatásáért hatás- és jogosultsági körére vonatkozóan minden érintett alkalmazott felelős;

- a szabályzatban előírtak betartásának ellenőrzése az ügyvezető igazgató feladata.

## 18. MEGISMERÉSI KÖTELEZETTSÉG:

- **A** szabályzat előírásait a Szekszárdi Vagyonkezelő Kft.-nél dolgozó minden személy a szakmai feladatköréhez szükséges mértékben köteles megismerni, a vonatkozó előírásokat betartani és betartatni.

- A szabályzat egyes előírásait, a munkavégzéséhez szükséges mértékben, minden, a Szekszárdi Vagyonkezelő Kft.-vel munkaviszonyban, illetve egyéb szerződéses jogviszonyban álló foglalkoztatottal ismertetni kell.

- A szabályzat előírásait megszegőkkel, illetve a jelentési kötelezettséget elmulasztókkal szemben, a hatályos törvényeknek, rendeleteknek és belső szabályzóknak megfelelő, jogszerű felelősségre vonást kell alkalmazni.

## 19. A SZEKSZÁRDI VAGYONKEZELŐ KFT. INFORMATIKAI, SZÁMÍTÁSTECHNIKAI ADATVÉDELME:

A Szekszárdi Vagyonkezelő Kft. számítástechnikai biztonságának - adatbiztonságnak - koncentrálódnia kell minden olyan, a Szekszárdi Vagyonkezelő Kft.-re és ügyfeleire vonatkozó tény, információ, megoldás vagy adat komplex védelmére, amelynek „házon belül” maradásához a Szekszárdi Vagyonkezelő Kft.-nek üzleti érdeke fűződik, szerződéses kötelezettséget vállalt, ill. jogszabály arra kötelezi.

- **Számítástechnikai** (logikai)- **adatbiztonság** körébe tartozik a számítástechnikai rendszer felépítése és működése; a külső- és belső rendszerfejlesztési tervek; az adatvédelmi előírások; a hozzáférési szintek, adat- és rendszertulajdonosi kijelölések; a számítógépes programok és nyilvántartások; az archiválási rendszer; a titokvédelem; a rendkívüli helyzetek kezelése, más országos informatikai rendszerhez csatlakozás; a híradástechnikai eszközök vonal- és titkosítási védelme; a szünetmentes tápellátás;
- **Egyéb irányú adatbiztonság** körébe tartozik a nem elektronikus adathordozók (iratok) tárolása;
- az információk adatok “kiszivárgásának” vagy „kiszivárogtatásának” megelőzése, illetéktelen hozzáférés megakadályozása, adatvesztés kizárása.

## 20. A SZEKSZÁRDI VAGYONKEZELŐ KFT. SZÁMÍTÁSTECHNIKAI ADATBIZTONSÁG OKTATÁSA:

20.1. A rendszerek oktatásának anyagi és technikai feltételeit az elméleti és gyakorlati oktatást az ügyvezető igazgató köteles biztosítani.

20.2. Az oktatásnak mindig szakterületeként differenciáltan kell történnie. A rendszer fejlesztésével (az ismeretanyag bővülésével) aktuálisan kell megtartani képzéseket, továbbképzéseket.

20.3. A képzéseket szükség szerint - a rendszer bonyolultságától függően - évente, ismeretfelelevenítő jelleggel meg kell ismételni.

20.4. Az oktatáson megjelenő személyek a képzés megtörténtét nyilatkozat formájában, aláírásukkal igazolják.

20.5. A Szabályzatnak a dolgozók részére - a feladatkörüket érintő mértékben - rendelkezésre kell állni.

# III. Fejezet

# Az Adatbiztonság alapelvei

## 21. ALAPELVEK ÉS BIZTONSÁGI FELTÉTELEK

21.1. Az informatikai fejlesztés teljes volumenét a projektvezető irányítja. A rendszer átvétele után a rendszergazda felügyeli és irányítja a vonatkozó tevékenységeket;

21.2. A Szekszárdi Vagyonkezelő Kft. szervezeti egységeinél csak a rendszergazdánál nyilvántartásba vett, és archivált szoftvereket (rendszereket) szabad alkalmazni;

21.3. Rendszert, - programot - verziószám nélkül kiadni tilos;

21.4. Fejlesztéshez csak jogtiszta, a rendszergazdánál nyilvántartásba vett szoftvereket lehet felhasználni;

21.5. A dokumentációk készítéséhez az egységes szövegszerkesztő és folyamatábra készítésére szolgáló programok használata kötelező;

21.6. A dokumentációk készítésénél a módosítások lapcserével történő megoldására kell törekedni;

21.7. Minden elkészült rendszert, illetve a vonatkozó dokumentációk egy példányát nyilvántartásába kell venni, és archiválni kell;

21.8. Az informatikai beszerzések és fejlesztések során a . üzletbiztonságát és titokvédelmét érintő szoftverek, nyilvántartások, adatbázisok és adatátviteli rendszerek kialakításánál törekedni kell a belső erőforrások felhasználására.

21.9. Vizsgálni kell a programhelyességet, valamint a dokumentációkat, az üzleti szakmai követelményeknek-, valamint ügyviteli szakmai-, továbbá a rendszerbiztonsági megfelelést;

21.10. Az elfogadott rendszert archiválni kell, és el kell készíteni a biztonsági- és tartalék példányokat, azokat a megfelelő biztonsági fokozattal kell tárolni;

21.11. A rendszert, vagy annak módosítását a rendszergazda telepíti;

21.12. Ugyancsak a rendszergazda felelőssége a számítógépes katasztrófa után a rendszer helyreállítása, ismételt installálása.

## 22. TERVEZÉS

A tervezés során a felhasználói igények és az erőforrások összehangolásán túl, a megvalósítási alternatívák kialakítása során törekedni kell a fejlesztési kockázat csökkentésére. A tervezés utolsó fázisaként elkészítendő számítástechnikai rendszertervnek minden esetben tartalmaznia kell a biztonsági - védelmi elemeket.

A rendszer-tervezés témaindító (előkészítő) megbeszélésébe az ügyvezető igazgatónak be kell vonnia a biztonságért felelős személyt (ha az nem a rendszergazda) vagy a rendszergazdát. A továbbiakban a rendszer tervezésébe biztonsági elemeket érintően a biztonságért felelős vezetőt a tervezés egyes fázisaiba a feladat volumene alapján és a kialakítandó rendszer ügyviteli minősítésétől függően kell bevonni.

Külső cég alkalmazottainak bevonása esetén, az ügyvezető köteles a tervezés megkezdése előtt a cégvezetés részére a külsős személyekről referenciákat kérni. A tervezés időszaka alatt a külső cég által delegált újabb személyekről is referenciát kell szolgáltatni.

Referenciák nélkül nem vonhatja be a külső cég alkalmazottait a tervezésbe.

A logikai rendszerterv minősítésétől függően, a résztvevőktől (amennyiben még nincs) nyilatkozatot kell venni.

22.1. Rendszerfejlesztés

A felhasználóknak minden esetben írásban kell jeleznie fejlesztési igényeiket. Az igénynek tartalmaznia kell a feladat megfogalmazását, a munkavégzők körét (szakmai színvonalát, informatikai képzettségét), a biztonsági elvárások szintjét és a teljesítés egyéb feltételeit.

22.2. A rendszer megvalósítása

A biztonságért felelős ügyvezetőnek abban az esetben is be kell tartatni a Szekszárdi Vagyonkezelő Kft. biztonságvédelmére vonatkozó szabályokat, ha a rendszer megvalósítása sürgős üzleti érdek;

A biztonságért felelős ügyvezető a rendszer minősítésétől függően, a rendszer biztonsági megfelelésének teszteléséhez külső szakértőket is bevonhat;

Amennyiben a biztonságért felelős ügyvezető a rendszer elemeit üzlet- vagy üzembiztonsági (adatvédelmi) szempontból nem tartja megfelelőnek, a rendszergazda a szükséges módosításokat köteles megtervezni és elvégezni;

Az integrációs teszt befejezésével a rendszernek olyan verziószámot kell adni, melynek az első számjegye a verziószámot, a második két számjegye pedig a verzión belüli változat számát jelöli.

A rendszer kialakítása és tesztelése során, a feladatokról és az értékelési eredményekről naplót (naplókat) kell vezetni;

A rendszer megvalósítása során keletkezett dokumentációkat és naplókat nyilván kell tartani, és minősítésének megfelelően kell kezelni;

## 23. A RENDSZER ÁTADÁS – ÁTVÉTELE

A rendszer átadás - átvétele csak az üzemszerű körülmények között hibátlanul működő teszt eredmények után engedélyezhető;
A vonatkozó dokumentációkat a rendszer átadásával egyidejűleg át kell adni a felhasználónak.

A rendszer átvétele során a felhasználó az igénye szerinti működőképes állapotot-, a rendszer minősítésének megfelelő biztonsági védettségét a biztonságért felelős ügyvezető aláírásával igazolja.

Olyan rendszert a felhasználónak kiadni tilos, amelynek logikai- és számítógépes rendszerterve, illetve maga a rendszer és annak felhasználói dokumentáció minden eleme nincs összhangban.

## 24. RENDSZER ÜZEMELTETÉSE

A rendszereket a Szekszárdi Vagyonkezelő Kft., mint a rendszer felhasználója üzemelteti. Felhasználók azok a személyek, akik a napi és időszaki tevékenységeket elvégzik.
A rendszert a Szekszárdi Vagyonkezelő Kft. szervezeti egységek a rendszer üzemeltetésével kapcsolatos észrevételeiket “Üzemeltetési Napló”-ban kötelesek vezetni.

A rendszergazda köteles a Szekszárdi Vagyonkezelő Kft.-vel folyamatosan kapcsolatot tartani és az észrevételekre a szükséges intézkedéseket megtenni;

A rendszer hibáit a rendszergazda köteles összegyűjteni. A vonatkozó fejlesztési javaslatokat és a fejlesztéssel kapcsolatos feladatokat az ügyvezető készíti el.

Az üzemelés során felmerült hiányosságok pótlását, a hibák kijavítását, illetve a szükséges módosítások és a vonatkozó dokumentációk elkészítését a rendszergazdának kell megtennie;

Az ügyvitelkövetésből adódó változtatások miatt minden esetben új rendszer-verziószámot kell adni;

Rendszerfejlesztési tevékenységet szigorúan a logikai rendszerterv megfelelő átdolgozásával kell kezdeni és minden változásnak új rendszer-verziószámot kell adni;

Minden végrehajtott módosítást a rendszer új verziószámával kell ellátni;

Minden új verzió vagy változat keletkezésekor gondoskodni kell a régi verzió záró adatainak átemeléséről az új változatba;

## 25. A RENDSZER LEÁLLÍTÁSA

A rendszer leállítását, a rendszert alkalmazó felhasználói környezet megszűnése, vagy olyan mértékű átalakítási igény okozhatja, amely teljesen új rendszer kialakítását igényli.

A rendszert, az üzemeltetési feltételek megszűnésével le kell állítani. A menteni szükséges adatokat az ügyvezető igénye alapján kell menteni, illetve azokat és a záró adatállományokat az érvényességi idő lejártáig (utódrendszer alkalmazása esetén is) archiválni kell.

A Szekszárdi Vagyonkezelő Kft. számára a továbbra is szükséges adatok mentéséről, az új rendszerbe történő átemeléséről, illetve a szabályzókban előírt archiválási kötelezettségek betartásáról, a rendszergazdának kell gondoskodnia.

## 26. A RENDSZERFEJLESZTÉS BIZTONSÁGI SZEMPONTBÓL LÉNYEGES DOKUMENTUMAI:

- Projektindítási jegyzőkönyv;
- Megvalósíthatósági tanulmány
- Logikai rendszerterv
- Számítógépes rendszerterv
- Forráskód, programozói dokumentáció
- Tesztelési dokumentáció
- Felhasználói dokumentáció

# IV. Fejezet

# Az informatikai hálózat és a hozzáférési jogosultságok

## 27. A SZEKSZÁRDI VAGYONKEZELŐ KFT. FIZIKAILAG ELKÜLÖNÜLŐ INFORMATIKAI TERÜLETEK

27.1. Adatbázisok, nyilvántartások
27.2. Távhőszolgáltatást igénybevevő szerződő partnerek/ lakóingatlan tulajdonosok vagy bérlők adatainak nyilvántartása,
27.3. Ügyfélszolgálati kommunikáció írásos rögzítése,
27.4. Statisztikák készítése,
27.5. Vezetői modul, a távoli kontrollhoz,
27.6. Számlázás,

27.7. Számlalevelek postázása,
27.8. Fénykép-felvételek tárolása.
27.9. Internetes és más külső kapcsolatot biztosító számítógépek;
27.10. A Szekszárdi Vagyonkezelő Kft. kommunikációs eszközei;
27.11. A Szekszárdi Vagyonkezelő Kft. egyéb tevékenysége keretében működő számítógépek.

## 28. A SZEKSZÁRDI VAGYONKEZELŐ KFT. SZÁMÍTÓGÉPES RENDSZERE:

**Virtuális szerver Windows 2008 Hyper-V**

Egy felhasználó > Administrator rendszergazdai jogosultsággal. Másnak nincs hozzáférése és ezen fut a két virtuális szerver.

Rendkívüli esemény, rendelkezésre állás hiánya miatti esetre zárt borítékban tárolva a hozzáférési és belépési azonosítók, jelszavak az ügyvezetőnél.

Virtuális szerver gép 1. Windows server 2012 op. rendszer, Parkolási rendszer és adatbázis, melyet az Atlas Kft. menedzsel. Egyben DHCP kiszolgáló is.

Virtuális szerver gép 2. Windows server 12012 op. rendszer, „Servantes" ügyviteli rendszer és adatbázis.

DNS kiszolgáló,

Felhasználói közös mappa,

Tartományvezérlés,

Felhasználói jogosultság vezérlő.

## 29. HOZZÁFÉRÉSI JOGOSULTSÁGOK:

29.1. a Microsoft programrendszer által használt valamennyi adatbázisba teljes betekintési joggal, a rendkívüli esetekben írási és módosítási joggal az ügyvezető igazgató, a rendszergazda és a könyvelési vezető rendelkezik;

29.2. a pénzügyi- és számviteli, továbbá a szabályozási- és fejlesztési, valamint a számítástechnikai rendszer adatbázisaiba a rendszergazdai munkakör betöltése esetén a rendszergazda teljes betekintési joggal rendelkezik;

29.3. a jelenlegi állapot, hogy az un. rendszergazdai tevékenységet az EPC plc, mint anyacég látja el, ezért az adatbiztonsági szabályzatot és a rendszergazda biztonsági feladatait a vállalkozói szerződéshez mellékleteként csatolni kell;

29.4. a hardware és software telepítésére, illetve módosítására kizárólag a rendszergazda adhat engedélyt;

29.5. a humánpolitikai, személyzeti anyagokhoz hatáskörileg a rendszergazda és a humánpolitikai feladatokkal megbízott alkalmazottak férhetnek hozzá;

29.6. az alkalmazottak a szabályzatban és a munkaköri leírásukban meghatározott adatbázisokhoz és nyilvántartásokhoz férhetnek csak hozzá.

## 30. A HOZZÁFÉRÉSI JOGOSULTSÁGOK BIZTOSÍTÁSA

30.1. Kétszintű belépési jogosultságokat kell biztosítani, az ügyvezető igazgató által jóváhagyott és meghatározott szinteknek megfelelően, azaz a felhasználók WINDOWS alapú hitelesítéssel azonosítják magukat a Windows rendszerhez való csatlakozáskor (belépéskor);

30.2. A belépési jogosultságot és hozzáférési szintet biztosító azonosítókat és jelszavakat a II. fejezet 8. pontokban meghatározott gépekhez az rendszergazdának kell beállítani;

30.3. Az új belépő dolgozót megfelelő csoportba sorolással minden általa használt gépre fel kell venni. A dolgozó saját névvel lép a hálózatba, majd az azonosítót és a belépési jelszót (jelszavakat) önállóan rögzíti a gépben;

30.4. A dolgozók tájékoztatása a hálózat használatával kapcsolatos kötelességeikről, jogaikról és lehetőségeikről, a rendszergazda kötelessége.

## 31. SZEKSZÁRDI VAGYONKEZELŐ KFT. RENDSZERGAZDA FŐBB FELADATAI:

31.1. A rendszergazdai feladatokat az Laptopdigital Kft. látja el karbantartási és javítási szerződés alapján, ezért az alábbi feladatok megvalósulásáért, végrehajtásáért az Laptopdigital Kft. vezetőjével és munkatársaival folyamatosan egyeztetni kell.

31.2. Gondoskodik az informatikai biztonsági rendszer kialakításáról, fejlesztéséről, az informatikai védelmi szolgáltatások biztosításáról és az ehhez kapcsolódó biztonsági előírások érvényesítéséről.

31.3. A biztonságvédelmi elvek figyelembevételével kialakítja, irányítja, szervezi és koordinálja a fonikus, digitális, valamint egyéb adatátviteli feladatköröket.

31.4. Biztosítja a titkosított adatátvitel feltételeit, illetve gondoskodik az ehhez szükséges eszközök rendelkezésre állásáról.

31.5. Gondoskodik a minősített adatok és információk, hozzáférési jogosultság szerinti kezelési feltételeinek megteremtéséről.

31.6. Tervezi, szervezi és koordinálja a rendkívüli eseményekre, illetve katasztrófa helyzetekre szóló informatika biztosítását, a Szekszárdi Vagyonkezelő Kft. adatainak, adathordozóinak védelmét, illetve szükség esetén megsemmisítési rendjét.

31.7. Irányítja az informatikai vonatkozású rendkívüli események kivizsgálását.

Az ügyvezető igazgató elláthatja a rendszergazdai egyedi, speciális feladatokat, amennyiben nem rendelkezik szakismerettel, külsős szakembert vagy szolgáltató céget megbízhat. Az írásos megbízásokban minden esetben rögzíteni kell a konkrét feladatokat és azok végrehajtásának módját, idejét és felelősét.

31.8. A hatályos jogszabályokat és a biztonsági követelményeket figyelembe véve, elkészíti és aktualizálja Szekszárdi Vagyonkezelő Kft. Adat-, és Számítástechnikai biztonsági Szabályzatát.

31.9. Gondoskodik az informatikai biztonsági rendszer kialakításáról, fejlesztéséről, az informatikai védelmi szolgáltatások biztosításáról és az ehhez kapcsolódó biztonsági előírások érvényesítéséről.

31.10. A biztonságvédelmi elvek figyelembevételével végrehajtja, kialakítja a fonikus, digitális, valamint egyéb adatátviteli rendszereket.

31.11. Ellenőrzi a titkosított adatátvitel feltételeit, illetve gondoskodik az ehhez szükséges eszközök rendelkezésre állásáról.

31.12. Kialakítja a minősített adatok és információk, hozzáférési jogosultság szerinti kezelési feltételeit.

31.13. A rendkívüli eseményekre, illetve katasztrófa helyzetekre vonatkozó előírások, tervek szerint biztosítja informatikai rendszer működőképességét, a Szekszárdi Vagyonkezelő Kft. adatainak, adathordozóinak védelmét, illetve szükség esetén megsemmisítési rendjét.

31.14. Minden hozzáférés loggolása az adatbázisokhoz,

31.15. Rendszerleállítás / indítás loggolása, (mivel leállítás után loggolás nélkül offline lenyerhetők az adatok)

31.16. A log-file-ok periódikus mentése és biztonságos helyen történő elhelyezése a későbbi esetleges visszakeresés biztosítása érdekében.

31.17. Végrehajtja az informatikai vonatkozású rendkívüli események kivizsgálását, megállapításait írásba foglalja.

31.18. A rendszer periodikus tesztelése a software-piacon elérhető minőségi biztonság-tesztelő programokkal,

31.19. Külső, internetes támadások elleni védelem biztosítása.

## 32. KÖTELEZETTSÉGEK A KATASZTRÓFAHELYZET MEGELŐZÉSÉBEN ÉS ELHÁRÍTÁSÁBAN:

A tartalék működési helyen, továbbá a mobil vezetési pontról, illetve helyről történő működéshez a feltételek biztosítása az ügyvezető igazgató feladata.

a) A számítógépes adatfeldolgozáshoz és összeköttetéshez (hardver; szoftver; elektromos tápegység), továbbá a híradástechnikai forgalmazáshoz (telefon; mobiltelefon; FAX) szükséges feltételeket;

b) a vezetés részére a számítógépes eszközöket, illetve számítógépes adathordozókon a rendkívüli események és a katasztrófa elhárításra vonatkozó valamennyi a Szekszárdi Vagyonkezelő Kft. által készített, illetve a vonatkozó magasabb szintű szabályzót.

**Általános kötelezettségek:**

a) Rendelkezni kell olyan informatikai katasztrófa-elhárítási feladat- és intézkedési tervvel, amellyel szükség esetén azonnal be tud avatkozni az informatikai katasztrófa-elhárítás tevékenységeibe, illetve amelyet a vezetés döntés előkészítéseihez és intézkedéseihez azonnal rendelkezésre tud bocsátani;

b) Biztosítania kell a rendkívüli időszaki tevékenységhez a jogszabályokban meghatározott, illetve a Szekszárdi Vagyonkezelő Kft. vezetése által kijelölt informatikai összeköttetések személyi és technikai feltételeit;

c) A katasztrófa-terv egy példányával írásban és számítógépes adathordozón minden vezetőnek rendelkeznie kell.

# V. Fejezet

# Adatvédelmi incidens

## 33. FOGALMA:

A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan kezelését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

## 34. INCIDENSEK BESOROLÁSA:

34.1. Bizalmassági incidens, amikor a személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy ezekhez való hozzáférés történik,

34.2. sértetlenséggel kapcsolatos incidens, amikor az adatok véletlen vagy jogtalan megváltoztatása történik,

34.3. hozzáférhetőséggel kapcsolatos incidens, amikor személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése következik be.

34.4. Az adatvédelmi incidens következményei a megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek:

- a személyes adatok feletti rendelkezés elveszítése,
- jogaik korlátozása,
- személyazonosság lopását vagy a személyazonossággal való visszaélés,
- pénzügyi veszteség,
- jó hírnév sérelmét,
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése.

## 35. INCIDENS-KEZELŐ CSOPORT:

Az adatvédelmi incidenst vizsgáló csoport döntést hozó vezetője a Szekszárdi Vagyonkezelő ügyvezető igazgatója,

tagjai:
adatvédelmi tisztviselő
Informatikai rendszergazda,
Vagyonkezelői jog gyakorlója (önkormányzat),
Vagyonkezelő műszaki igazgatója
Az érintett terület részéről - ahol az incidens bekövetkezett - az első számú vezető, vagy részleg vezetője (HR, IT, Ügyfélszolgálat),

## 36. AZ INCIDENS KEZELÉSÉVEL ÖSSZEFÜGGŐ FELADATOK:

- ✓ incidens azonosítása,
- ✓ incidens minősítését bizonyító adatok, dokumentumok vizsgálata,
- ✓ incidens által bekövetkezett kockázat, kár, veszélyhelyzet meghatározása,
- ✓ elhárítás érdekében teendő intézkedések meghatározása,
- ✓ incidens bejelentésére vonatkozó döntés meghozatala,

- ✓ incidens okainak feltárása,
- ✓ érintettek tájékoztatása,
- ✓ teljes vizsgálat megindítása igény szerint,
- ✓ kapcsolattartás a NAIH-val.

## 37. ADATVÉDELMI INCIDENS AZONOSÍTÁSA, MINŐSÍTÉSE, TÍPUSA:

A biztonságnak olyan sérülése, amely által a tárolt, továbbított vagy más módon kezelt adatok véletlen vagy jogellenes módon megsemmisül, elvész, megváltozik, jogosulatlanul közlésre kerül, vagy jogosulatlan hozzáférést eredményez.

- Személyes adatok feletti rendelkezés elvesztése,
- jogok korlátozása,
- hátrányos megkülönböztetés,
- személyazonosság-lopás vagy azzal való visszaélés,
- pénzügyi veszteség,
- az álnevesítés engedély nélküli feloldása,
- jóhírnév sérelme,
- titoktartási kötelezettség megszegése által bizalmas jelleg sérülése,
- gazdasági vagy szociális hátrány.

Az azonosítást követően a minősítés érdekében tisztázni kell az alábbiakat:

- Milyen kockázatot jelent az érintett természetes személy(ek) jogaira és szabadságaira tekintettel.
- Kiváltó okok, körülmények, amelyek az incidens bekövetkezéséhez vezettek. Az incidens bekövetkezésének körülményei.
- A személyes adatok érzékenységének meghatározása,
- Az incidensben érintett személyes adatok száma.
- Az érintett adatok fajtái, ill. az érintetti kör speciális tulajdonságai.

## 38. ADATVÉDELMI INCIDENS JELENTÉSE:

38.1. Az adatvédelmi incidenst az érintett tagvállalat vagy részleg, ill. az adatfeldolgozó a tudomására jutást követően indokolatlan késedelem nélkül azonnal jelenti az adatvédelmi incidenst kezelő csoport valamely állandó tagjának;

38.2. Ismertetnie kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

38.3. Közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

38.4. Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

38.5. Ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;

38.6. A csoport döntése alapján bejelenti az adatvédelmi incidenst (legfeljebb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott), a GDPR 55. cikk alapján illetékes felügyeleti hatóságnak, NAIH-nak.

38.7. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

38.8. Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor nem kell bejelentenie a hatóságnak, de az incidenst nyilvántartásba kell venni.

38.9. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

## 39. AZ ÉRINTETT TÁJÉKOZTATÁSA AZ ADATVÉDELMI INCIDENSRŐL:

- Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
- Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az intézkedéseket is.
- Az érintettet nem kell tájékoztatni, ha az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.
- Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását.

## 40. AZ ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA:

Az adatvédelmi nyilvántartás a NAIH által ajánlott és kitöltött bejelentő lapok (Melléklet) alapján, azok iktatásával és elektronikus másolatának tárolásával valósul meg, mely a teljes felsorolás nélkül az alábbiakat tartalmazza:

- az incidens jellege, az adatvédelmi incidenshez kapcsolódó tények, annak hatásai,
- érintettek kategóriái és száma,
- adatok kategóriái és száma,
- valószínűsíthető következmények,
- az incidens következményei elhárítására, következmények enyhítésére tett és tervezett intézkedések,

Az adatvédelmi incidensek nyilvántartását az adatvédelmi tisztviselő/felelős vezeti elektronikus dokumentumban, excel táblázatban.
A nyilvántartás része az incidenssel kapcsolatos vizsgálódás dokumentumának elektronikus másolata.
Az incidens vizsgálatát és kezelését - a NAIH honlapjáról letölthető - papíralapú incidens-bejelentő lap (Melléklet) kitöltésével kell dokumentálni.

### 41. KOCKÁZATÉRTÉKELÉS SZEMPONTJAI:

- az incidens típusa,
- a személyes adatok típusa és mennyisége,
- az érintettek azonosíthatóságának lehetősége,
- a következmények súlya az érintettekre nézve – kategóriái, száma,
- a következmények súlya az adatkezelőre nézve (speciális kategória).

## VI. Fejezet

## A Szekszárdi Vagyonkezelő Kft. informatikai rendszereinek vírusfertőzés és külső behatolás elleni védelmének feladatai

A vírus és külső behatolás elleni védelem a Szekszárdi Vagyonkezelő Kft. adatvédelmi rendszerének elengedhetetlenül szükséges biztonsági eleme.

A számítógépes vírusok és külső behatolások elleni védelem lehetőségeinek, illetve a vírusok elhárításának a számítógépes rendszernél alkalmazott módszereit, illetve a jelen szabályozásban leírt követelményeket valamennyi felhasználónak alkalmazási szinten kell ismernie.

### 38. A VÍRUSOK ELLENI VÉDELEM:

#### 38.1. A vírusok keletkezésének (rendszerbe kerülésének) oka:

- A vírus olyan program (programrészlet) amely képes arra, hogy reprodukálja magát (önmagát másolva “szaporodjon”), így az éppen alkalmazásban lévő programokhoz kapcsolódva, különböző rendellenességeket, károkat okozzon.
- A vírusok általában idegen, a rendszerben ellenőrzés nélkül használt, már fertőzött adathordozókról (hajlékony- vagy merevlemez, CD) történő beolvasás során kerülnek a számítógépes rendszerbe, továbbá bekerülhetnek a számítógépes hálózaton át is.
- A vírus továbbterjedése a fertőzött objektum aktivizálódása után, a vírus típusától függő metódus szerint történik

#### 38.2. A vírus aktivizálódására utaló jelek:

- indokolatlan és értelmezhetetlen hibaüzenetek, szövegek megjelenése;
- szokatlan hang- vagy fényeffektusok;
- dokumentumok, táblázatok, adatbázisok helyrehozhatatlan károsodása;
- programok működési funkcióinak megváltozása, funkciók eltűnése, méretének megváltozása;
- gyakori “lefagyások”;

- a tartalomjegyzék “összekeveredése”;
- az operációs rendszer meghibásodása, esetleg “eltűnése”;
- a számítógép műveleteinek szembetűnő lelassulása.

**38.3. A vírusfertőzések elkerülésének megelőzési módszerei:**

A vírusokkal szemben, azok folyamatos “fejlesztése”, illetve újak kifejlesztése miatt, elvileg nem létezik teljes védelem, ezért kiemelt jelentőségű a megelőzés, a felhasználók által a vonatkozó informatikai biztonsági szabályok betartása.

- hatékony szoftveres és hardveres eljárások bevezetése;
- a felhasználók felkészítése a vírus elleni védelemre, a vonatkozó szabályok megismertetésén, és betartásának megkövetelésén keresztül.

**38.4. A vírusfertőzések elkerülésének megelőzési szabályai:**

- Valamennyi számítógépen, illetve számítógépes rendszeren, az előírásoknak megfelelően be kell tartani a mentéseket;
- Kizárólag jogtiszta, ellenőrzött és bevizsgált szoftverek használhatók;
- Az alkalmazott szoftverekről minden esetben biztonsági másolatot kell készíteni és a telepítést minden esetben a másolatról kell készíteni;
- Az eredeti szoftvert tartalmazó adathordozót fizikailag elkülönített helyen, tűzbiztos szekrényben kell tárolni;
- A számítógép bekapcsolásakor floppy nem lehet a meghajtóban; floppyt a meghajtóban csak felhasználása idejéig szabad tartani;
- A számítógép rendellenes működése esetén vírusellenőrzést is kell végezni;
- Minden egyes felhasználásra beérkező, illetve kimenő adathordozót vírusvizsgálati eljárásnak alávetni;
- Új programot (vagy verziót) kizárólag a rendszergazda, ill. számítógépes szakember telepíthet;
- Valamennyi beépített merevlemezzel rendelkező számítógépen naponta, az első indításkor automatikus vírusellenőrzésnek kell lefutnia; Minden újraindításkor a memóriát kell ellenőrizni;
- Valamennyi szerveren állandó vírusellenőrzésnek kell működnie;
- A felhasználói munkaállomásokon, amennyiben a hardver lehetővé teszi, a floppylemezről történő indítást le kell tiltani;
- A felhasználók kizárólag a Szekszárdi Vagyonkezelő Kft. vezetője által meghatározott vírusellenőrzési eljárásokat alkalmazhatják;
- Az Internet használata során beérkező, letöltött állományokat kizárólag vírusellenőrzés után szabad felhasználni.

**38.5. Az automatikus vírusellenőrzési rendszereket kikapcsolni, illetve azokat megkerülni tilos!**

**38.6. A vírusfertőzésre utaló bármilyen jelenséget azonnal jelenteni kell:**

- a közvetlen vezetőnek,
- az adatvédelmi tisztviselőnek,
- a rendszergazdának, és a Help Desk szolgálatnak,

**A felhasználók további intézkedésig a vírusgyanús gépet nem használhatják.**

### 38.7. A vírusvédelmi szoftverek használatának biztonsági szabályai:

a. A szoftverek telepítése

A vírusvédelmet biztosító szoftverek telepítése, frissítése központilag, a rendszergazda által történik;

A telepítésre kerülő számítógépeken mindig a legfrissebb vírusellenőrzési eljárást kell alkalmazni;

b. A szoftverek üzemeltetése

Valamennyi winchesterrel rendelkező PC gépen bekapcsoláskor és új rendszerindításkor naponta le kell futnia az automatikus vírusellenőrzésnek, amely egyidejűleg az ellenőrzés eredményét file-ba rögzíti. A vírusellenőrzési jelentésfile-ok tartalmát havi rendszerességgel összesíteni kell.

A fiókok részére az informatikai rendszernek megfelelő vírusellenőrző rendszert kell biztosítani.

### 38.8. A vírus és külső behatolás elleni védelem felügyelete a rendszergazda feladata és felelőssége:

A rendszergazda feladatai és felelősségi köre:

- Kísérje figyelemmel a vírusellenőrzési programok, eljárások irodalmát, tegyen javaslatot hatékony módszerek bevezetésére;
- Irányítsa és felügyelje a vírusellenőrzők új verzióinak telepítését;
- Tegyen javaslatot a vírusellenőrzési eljárások szabályozására;
- vírusfertőzések esetén vizsgálja ki a fertőzés eredetét, hozzon intézkedést az újabb fertőzés elhárítására;
- Tartsa nyilván a Szekszárdi Vagyonkezelő Kft. birtokában lévő vírusvédelmi eszközöket, regisztrálja az újabb verziók beérkezését, azok telepítését;
- Tartsa nyilván a vírusfertőzéssel és eltávolítással kapcsolatos dokumentumokat;
- Havonta készítsen összegző értékelést, illetve beszámoló jelentése;

## 39. AZ ÜGYVEZETŐ IGAZGATÓ VÉDELEMMEL KAPCSOLATOS FELELŐSSÉGE

Az ügyvezető igazgatónak a vírusfertőzés megelőzésére minden lehetséges intézkedést meg kell tenni. Rendszeresen meg kell győződnie arról, hogy a beosztottak, számítógépet használók a védelmi szabályokat betartják-e.

- **A vírusvédelemmel kapcsolatosan alkalmazni kötelező okmányok:**

A víruskereső felhasználói leírása;
Vírusellenőrzési jegyzőkönyv a beérkezett- illetve kimenő adathordozók ellenőrzéséről;
Jegyzőkönyv a vírusfertőzésről.

A vírusfertőzés és incidens jegyzőkönyvének vezetésére kötelezett: a rendszergazda

| Sorszám | Dátum | Beérkezett / Kimenő | Adattartalom megnevezés | Illetékes szervezeti egység |
|---|---|---|---|---|
| | | | | |

**Jegyzőkönyv vírusfertőzésről, adatvédelmi incidensről**

| | |
|---|---|
| A vírusfertőzés és incidens észlelésének ideje | |
| A vírusfertőzés és incidens észlelésének helye (szervezeti egység) | |
| A számítógép leltári száma | |
| A fertőzés és incidens észlelése | |
| A fertőzés és incidens oka | |
| Az érintett egyéb rendszerek, gépek | |
| A mentesítés módja | |
| A használt vírusirtók | |
| Egyéb megjegyzés | |

Hely: Dátum:

A mentesítést végezte és ellenőrizte:

| Név (olvasható), beosztás | Aláírás |
|---|---|

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## VII. Fejezet
## FOGALMAK, ÉRTELMEZÉSEK

**Az üzleti titok fogalma:**

A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény 4. §-a (3) bekezdésének a) pontja határozza meg az üzleti titkot, amely „a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a **szükséges intézkedéseket megtette**".

Ezt erősíti meg a Btk. 300. §-a, amely az üzleti titok védelméről rendelkezik. A Btk. „a büntetőjogi védelmet kizárólag azokra az üzleti titkokra terjesztette ki, amelyeknek titokban maradásához a jogosultnak nemcsak, hogy méltányolható érdeke fűződik, hanem a szükséges intézkedéseket meg is tette az üzleti titok titokban tartása érdekében. Az intézkedések körében a legkézenfekvőbb az **üzleti titokká minősítés**, de e körbe tartozik minden olyan ésszerű és szükséges intézkedés, amely az üzleti titok megőrzése érdekében indokolt".

Tehát a menedzsment csak akkor bízhat joggal abban, hogy az üzleti tikok megsértőivel szemben (jogi) védelemben részesül, ha bizonyítani tudja, hogy minden ésszerű intézkedést megtett az üzleti titkok megőrzéséhez.

Adatvédelem

Az információs önrendelkezési jogról és az információszabadságról1 (röviden adatvédelmi törvény) szóló 2011. évi CXII. törvény szerint az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, **köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.** Az adatokat – kiemelten az államtitokká és a szolgálati titokká minősített személyes adatot – védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

**Adat- informatika-biztonság:**

Az adatok bizalmasságának, hitelességének és sértetlenségének biztosítása. A megbízható működés érdekében az informatikai rendszer hardware és szoftver eszközeinek folyamatos rendelkezésre állása és funkcionalitása.

**Bizalmasság:**

A titokvédelmi szempontból lényeges értékek, adatok védelme a jogosulatlan felfedés ellen.

**Információ:**

Az adat, az adatállomány szerkezete, a kezelésére vonatkozó szabályok, eljárások és az adathordozó együttesen.

**Logikai védelem:**

Az értékekhez és információkhoz való szándékos vagy véletlen illetéktelen hozzáférés, megváltoztatás és megsemmisítés ellen alkalmazott eszközök, eljárások és módszerek alkalmazása.

**Kockázat:**

A veszélyforrások által okozható károk bekövetkezésének lehetősége, amely az intézménynél veszteséget vagy szolgáltatási, működési zavarokat okozhat.

**Felhasználói kézikönyv:**

A rendszerindítás és a rendszerzárás közötti műveletek, menük, a rendszer által támogatott, vagy megvalósított folyamatok (tranzakciókat) szabatos leírását tartalmazza.

Tartalmazza továbbá a felhasználó számára kezelhető módon, a felhasználói hibákból való kivezetések lehetőségeit és az informatikai biztonsági - védelmi előírásokat.

**Üzemeltetési kézikönyv:**

A rendszer szabályszerű indításához és lezárásához, valamint a meghatározott időszakonként végzett tevékenységek (mentések, archiválások) végrehajtásához szükséges műveleteket írja le.

**Rendszergazda kézikönyv:**

A rendszergazda részére készül. Az adatbázisok szerkezetét, a programok összefüggéseit és logikai sémáját, valamint a lehetséges hibák okait és következményeinek leírását tartalmazza.

**Ügyviteli leírás:**

Azon szakmai terület szaknyelvű leírása, amelynek részleges vagy teljes támogatására az adott informatikai rendszer készült.

**Help Desk szolgálat:**

A számítástechnikai központ munkatársai által ellátott, szolgáltatás-jellegű tevékenység (felhasználói problémák kezelése).

**Help Desk napló:**

A HelpDeskhez érkező felhasználó bejelentések, információk, továbbá az azokkal kapcsolatos események rögzítésére szolgáló napló. A naplózást az Számítógépközpont vezetője végzi.

**Függő ügy:**

Minden önálló tárgyú bejelentés és információ, amely további intézkedéseket igénylő ügy, a befejezéséig.

**Rendelkezésre állás:**

Annak biztosítása, hogy az erőforrás az eredeti szolgáltatásokat folyamatosan és rendeltetésszerűen nyújtsa ott és akkor, amikor és ahol szükség van rá.