E-12/2017

ADATVÉDELMI SZABÁLYZAT és INFORMATIKAI HÁZIREND 2017

Cég neve:	Balatoni Integrációs Közhasznú Nonprofit Kft.
Címe:	8600 Siófok, Batthyány u. 1.
Adószáma:	20638119-2-14

Képviseletre jogosult személy(ek) neve: Dr. Molnár Gábor ügyvezető igazgató

Jelen szabályzatban nem szabályozott kérdésekben a számviteli törvény és a kapcsolódó jogszabályok vonatkozó előírásai szerint kell eljárni. Felülvizsgálata és karbantartása a jogszabályi változások függvényében, de legalább évente történik.

Hatályba lépett: 2014. 12. 21 -án/-én

a cég képviseletére jogosult személy(ek)
cégszerű aláírása

1. A szabályzat célja

Jelen dokumentum célja a Balatoni Integrációs Kft. adatvédelmi kérdéseinek szabályozása. Alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és azok jogosulatlan nyilvánosságra hozatalát.

Célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- a telepített számítástechnikai eszközök és programok illetéktelen felhasználás elleni védelme,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- a védett adatokhoz való illetéktelen hozzáférés, változtatás és nyilvánosságra hozatal elleni védelem,
- az adatok fizikai megsemmisülésének minden lehetőségétől való védelme,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzat az adatvédelem általános érvényű előírását tartalmazza. Meghatározza az adatvédelem és adatbiztonság feltételrendszerét. Célja továbbá az új felhasználók tájékoztatása az informatikai szolgáltatások igénybevételének és az eszközök használatának alapvető szabályairól.

2. A szabályzat hatálya

2.1. Személyi hatálya

- kiterjed a Társaság valamennyi cégi egységére, alkalmazottjára valamint a Társasággal szerződéses viszonyban álló, informatikai rendszereit használó személyekre.

2.2. Tárgyi hatálya

Tárgyi hatálya kiterjed:

- a Társaság tulajdonában lévő, illetve az általa bérelt valamennyi informatikai eszközre, azok műszaki dokumentációira,
- a számítógépes rendszer teljes konfigurációjára, az ahhoz tartozó rendszer- és felhasználói programokra, valamint ezek dokumentációira;
- a számítástechnikai eszközök alkalmazásának teljes folyamatára, tevékenységeire;

- a számítógépes feldolgozásra szánt, feldolgozás alatt álló, és a feldolgozás után a számítógépes adathordozókon tárolt, illetve a feldolgozás eredményeként létrejött adatokra;
- a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül.

A munkatársak személyesen felelnek a Társaság anyagi és szellemi értékeinek megőrzéséért.
A cég vagyonát érintő sérelemről vagy a sérelem bekövetkezésének közvetlen veszélyéről a közvetlen felettest azonnal tájékoztatni kell.
Jogszabályba ütközik - ezért kártérítési felelősséggel jár - minden olyan, a cég vagyoni érdekeit sértő magatartás, amely nemcsak a munkatársaktól elvárt viselkedés normáit sérti, hanem a Társaságnak kárt is okozhat.
Külső cégek munkatársai által végzett tevékenységért a Balatoni Integrációs Kft. oldali szerződéskötő, illetve kapcsolattartó a felelős. Külsős felhasználó esetén figyelni kell arra, hogy az igényelt, illetve kiadott jogosultság nem haladja-e meg a munkája elvégzéséhez szükséges mértéket.

3. Az adatkezelés során használt fontosabb fogalmak

Adat: Az információ konkrét megjelenési formája, számítógép által kezelhető szimbólumok összessége.

Adatalany / érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

Adatátvitel: Adatok elektronikus úton történő átadása számítógépek között.

Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere. 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 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.

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi.

Adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

Adathalászat (phishing) - Adathalászatnál egy jól ismert weboldalt (pl. bank) másolnak le a csalók, ahol arra próbálja rávenni a felhasználót, hogy adják meg személyes, és titkos adataikat. Ehhez egy e-mailt küldenek körbe, melyben kérik, hogy a lemásolt oldalt nézzék meg.

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala,

összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi.

Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

Adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

Adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Belső adatvédelmi felelős: az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős.

Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Biztonság: Az előírások és szabványok betartása az információk rendelkezésre állásának, sértetlenségének, bizalmasságának vagy hitelességének, valamint a rendszer működőképességének megtartása érdekében.

Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

Célhoz kötött adatkezelés: személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és - ha az adatkezelés céljára tekintettel szükséges - naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

Cloud computing: („számítástechnikai felhő", „felhő alapú informatika"): a számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (pl.: Gmail), vagy az online tárhelyek (pl.: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.

Cookie-k („sütik"): rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat [kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek] csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetőek a felhasználó böngészési szokásai.

Európa Tanács Adatvédelmi Egyezménye: az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény (az Európa Tanács ún. 108-as Egyezménye). Az első jelentős, az aláíró államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Magyarországon kihirdette az 1998. évi VI. törvény, 1998. február 27-én.

Érintett: bármely meghatározott, személyes adat alapján azonosított – közvetlenül vagy közvetve – azonosítható természetes személy.

Érintett jogai: az adatalanyt még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor egyértelműen tájékoztatni kell az adatkezelés minden részletéről. Az érintett kérheti adatai helyesbítését, bizonyos esetben törlését is, valamint törvényben meghatározott esetekben tiltakozhat személyes adatai kezelése ellen.

Felhasználó: Az a személy vagy szervezet, aki (amely) egy vagy több alkalmazói programot használ feladatai megoldásához.

Felügyeleti szoftver (felügyeleti rendszer): Az informatikai rendszer működésének ellenőrzésére, az adatbiztonság felügyeletére szolgáló szoftver.

Férgek: olyan programok, amelyek képesek reprodukálni magukat, de terjedésükhöz a vírusokkal ellentétben nem szükséges hordozóközeg, mivel a számítógépes hálózatokat felhasználva terjednek. A gyors terjedésük miatt a legveszélyesebb programok ebből a típusból kerülnek ki. Mire egy-egy újabb féreg jelenlétét észrevennék, és az ellenszert elkészítenék az

erre szakosodott cégek, addig a féreg az internetet használva akár több százezer gépet is képes megfertőzni. Sokféle kárt képes okozni, de már a terjedéssel is sávszélességet foglal, vagyis az internet egyéb, hasznos forgalmát hátráltatja.

GDPR: (General Data Protection Regulation) uniós általános adatvédelmi rendelet.

Hálózat: A rendszerben lévő központi eszközöket és a munkahelyi számítógépeket a központtal és egymással fizikailag összekapcsoló vonal, amely az informatikai rendszerekben az adattovábbítást lehetővé teszi.

Hardver: Az informatikai rendszer adatbevitelt, adatfeldolgozást, adattárolást és adattovábbítást végző fizikai elemei.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

Hozzáférés: Olyan eljárás, amely valamely informatikai rendszer felhasználója számára elérhetővé teszi a rendszerben az adatokként tárolt információkat.

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Információ: Olyan adat, hír vagy közlés, amely a címzett részére közvetlenül vagy további feldolgozás útján értelmezhető, újdonságot hordoz.

Információszabadság: a közérdekű, valamint közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, mely elősegíti a közhatalom gyakorlásának demokratikus kontrollját és a közintézmények átláthatóságát (transzparencia).

Infotv.: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, amelyet az Alaptörvény VI. cikke alapján az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, az ezen jogok érvényesülését szolgáló alapvető szabályokról, valamint az ellenőrző hatóságról (NAIH) alkotott. A törvény célja, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon. 2012. január 1-től hatályos.

Kémprogramok: Feladatuk a gépen tárolt bizalmas adatok (jelszavak, kódok, bankkártya- és személyes adatok) megszerzése, és továbbítása. Sok kémprogram azt figyeli, hogy a felhasználó milyen tartalmú weboldalakat néz az interneten, és az így megszerzett információ alapján célzott reklámokat, hirdetéseket küld a felhasználó gépére.

Kötelező szervezeti szabályozás: több országban, de köztük legalább egy EGT-államban is tevékenységet folytató adatkezelő vagy adatkezelők csoportja által elfogadott és a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) által jóváhagyott, az adatkezelőre vagy adatkezelők csoportjára nézve kötelező belső adatvédelmi szabályzat, amely a harmadik országba történő adattovábbítás esetén a személyes adatok védelmét az adatkezelő vagy adatkezelők csoportjának egyoldalú kötelezettségvállalása útján biztosítja.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére

vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Központi számítógép (szerver): Olyan nagy kapacitású számítógép, amely a számítógépes hálózat csomópontjaként lehetővé teszi a hálózatba kapcsolt ügyfél számítógépek (kliensek) számára a központi számítógép erőforrásainak használatát.

Különleges adat:
a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Láncievél – *hoax* - A láncievél egy hasznot nem hozó, sőt sokszor bosszantó e-mail fajta. Ez az a levél, ami arra kéri olvasóját, hogy minél több példányban küldje tovább. Ennek érdekében általában az érzelmekre próbál hatni, vagy áltudományos adatokra hivatkozik. Káros tevékenysége ugyan nincs, az elolvasásával és továbbküldésével töltött időt más, fontosabb tevékenységtől vesszük el.

Megfelelő tájékoztatás: az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá 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, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Munkahelyi számítógép: A munkahelyre telepített személyi számítógép, notebook vagy munkaállomás.

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

Shareware: Olyan szoftver, melynek másolása megengedett, ám a használatuk korlátozott. A korlát vonatkozhat a szoftver képességeire, a felhasználók körére, vagy a felhasználási időre.

Spam - *Kéretlen reklámlevél* - Legtöbbször teljesen felesleges, a fogadó által nem kért, mégis nagy számban elküldött reklám, ami jelentősen terheli az internetet, foglalja a sávszélességet.

Számítógépes kártevők: A számítógépes kártevőknek sokféle fajtája létezik. Definíció szerint ezek olyan programok, amelyek nem hasznos tevékenységet folytatnak. Az angol elnevezésük malware, ami rosszindulatú programot jelent. Fajtái: vírusok, férgek, trójai programok, kémprogramok, egyéb káros program, és tevékenység (hoax, spam, adathalászat).

Személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Szoftver: Olyan szellemi termék, amely a számítógépes rendszer hardvertől különböző, meg nem fogható, nem fizikai része, és a rendszer által végrehajtható program(ok)ból áll, melyek feladata a hardver elemek összehangolt működésétől az adatfeldolgozásig terjed.

Szoftver eredetiséget igazoló tanúsítvány: Az OEM forgalmazók által a számítógépekkel közvetlenül vagy közvetve forgalmazott termékekhez járó biztonsági eszköz. Az eredetiséget igazoló tanúsítvány tanúsítja a vevő számára, hogy a számítógépéhez kapott program eredeti.

Szoftver felhasználói licence-szerződése: A licence-szerződés a jogilag tiszta úton beszerzett szoftver használatára vonatkozó megállapodás, amely a terméknek a felhasználó számítógépén történő használatát illetően meghatározott jogokat biztosít.

Szoftver használata: A szoftver akkor van "használatban" egy számítógépen, ha megtalálható azon a tartós tárra telepítve vagy a RAM memóriába töltve. Hálózati gépnél a szoftver kétféle módon lehet használatban: a számítógép merevlemezére telepített szoftver helyben történő futtatásával vagy a hálózati szerverre telepített szoftvernek a szerveren kívül történő futtatásával.

Szoftver, illegális: Illegális az a szoftver, amelynek a licence-szerződésben leírt használati feltételeit vagy a társaság által hozott szabályokat a felhasználó nem tartja be.

Szoftver jogszerű eredete: Jogszerű egy szoftver eredete és használata, ha a használatba vétel megfelel a szoftver licencében megfogalmazottaknak, illetve a társaság által hozott szabályoknak. A jogszerű eredet lehet kereskedelmi szoftver megvásárlása, szabadon terjeszthető szoftverek letöltése, shareware programok használata és számítógép-alkatrészekkel forgalmazott szoftverek használata.

Szoftver jogszerű eredetének igazolása: A szoftver eredetét igazolja a felhasználói licence-szerződés, a birtokbavételi igazolás (számlamásolat), és - amennyiben van - a felhasználói kézikönyvek, a telepítő-készletek és az eredetiséget igazoló tanúsítvány.

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

Trójai programok: olyan programok, amelyek önmagukban nem okoznak kárt, de segítik egyéb ártó szándékú programok bejutását, és működését a számítógépen. Mivel gyakran hasznos programnak mutatják magukat, ezért leggyakrabban a felhasználó tölti azt le számítógépére. Emellett terjedhetnek adathordozókon és e-mailben is.

Vírusok: olyan programok, melyek képesek reprodukálni, sokszorosítani önmagukat és terjedésükhöz bizonyos közegre van szükségük, mely nélkül működésképtelenek. Nem feltétlenül okoznak kárt, sokszor csak kisebb bosszantó tevékenységet művelnek. Először megpróbálnak minél jobban elterjedni, minél több gépet megfertőzni, majd egy esemény bekövetkezésekor (pl. adott időben) fejtik ki káros tevékenységüket. Ez lehet adatok törlése, felülírása, teljes adatmegsemmisítés, programok eltüntetése, esetleg hardvereszközök tönkretétele.

A vírusoknak három nagy fajtáját különböztetjük meg:

- *Állomány, vagy programvírus.* Ez a vírus állományokhoz kapcsolódik, ami leggyakrabban egy program. Ez az állománnyal együtt terjed egyik gépről a másikra. Amikor a program elindul, akkor aktiválódik a vírus is. Ha ezután további programokat indítunk el, akkor a vírus azokat is megfertőzi. Működése többnyire adott operációs rendszerhez, és bizonyos állománytípushoz (pl. exe) kötött.
- *Bootvírus* Nevét onnan kapta, hogy a háttértárolók meghatározott részére, az úgynevezett boot (betöltő) szektorba írja be magát. Ezt a boot szektort minden számítógép indításakor megvizsgálja a BIOS, és ha itt programot talál, akkor elindítja azt. Tehát ha egy vírus itt

helyezkedik el, akkor minden indításnál automatikusan az is aktiválódik, még a vírusirtó programok betöltődése előtt.

- *Makróvírus* A makrók olyan apró programok, melyek az ismétlő feladatokat automatizálhatják. pl. Microsoft Office csomag elemeiben (Word, Excel) is A makróvírus olyan program, ami ezekben a nagyobb programokon belül életképesek. Általában dokumentumokhoz csatolják magukat, és azokkal együtt terjednek. Ha megnyitjuk a dokumentumot, akkor elindul a vírus is.

Vírusokból az utóbbi időkben egyre kevesebb van, mivel már kevésbé hatékonyak az újabb, modernebb károkozókhoz képest.

VPN: (Virtual Private Network) virtuális magánhálózat, biztonságos saját hozzáférést biztosít a hálózathoz.

4. Kapcsolódó szabályozások, hivatkozások

Jelen szabályzat előírásai összhangban vannak:

- a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,
- az 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során (az Európa Tanács tagjai között Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről),
- az Iratkezelési szabályzattal,
- a Leltározási és értékelési szabályzattal,
- a Számviteli politikával.

5. Az Adatvédelmi Szabályzat és Informatikai Házirend alkalmazásának módja

Az Adatvédelmi Szabályzat és Informatikai Házirend előírásainak betartása - szükség szerint megismertetése - valamennyi alkalmazottra nézve kötelező.
A felhasználó köteles tudomásul venni, elfogadni, és magára nézve kötelező érvényűnek tekinteni a jelen Adatvédelmi Szabályzat és Informatikai Házirend előírásait, valamint az adatkezelésre vonatkozó tájékoztatást, melyet az 1. sz. mellékletben foglalt Felhasználói nyilatkozat aláírásával tanúsít.
A társaságnál adatkezelést végző alkalmazottak és a társaság megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottai kötelesek a megismert személyes adatokat üzleti titokként megőrizni.
A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek titoktartási nyilatkozatot (2. sz. melléklet) kötelesek tenni.

5.1. Az Adatvédelmi Szabályzat és Informatikai Házirend karbantartása

Jelen szabályzatot az informatikában - valamint a Társaságnál - a bekövetkező változások miatt időközönként aktualizálni kell. A szabályzat karbantartása az informatikai vezető útmutatása alapján az adatvédelmi felelős feladata.

5.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a cégi egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

Az adatok feldolgozásakor meg kell határozni a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára.

6.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

7. A védelem felelősei

A védelem felelőse a mindenkori informatikai vezető, a belső adatvédelmi felelős és a rendszergazdák. A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Társaság vezetőinek kell gondoskodnia.

7.1. Adatvédelmi felelős feladatai

Az adatvédelmi felelőst az ügyvezető bízza meg. Munkáját valamennyi munkatárs köteles segíteni. Tevékenységét a Társasággal megbízásos jogviszonyban lévő informatikusokkal együttműködve végzi (Átalánydíjas számítógép karbantartási szerződés, Átalánydíjas fájlszerver és backupserver karbantartási szerződés stb.)
Az adatvédelmi felelős köteles gondoskodni:

- a jelen szabályzat kezeléséről, naprakészen tartásáról, a módosítások átvezetéséről,
- a számítógépen kezelt, valamint a papír alapú, illetve hangfelvételen lévő adatállomány fizikai megsemmisülés elleni védelméről,
- a számítógépes rendszerben alkalmazott adatkezelési eljárások és az adatállományok biztonságáról,
- az illetéktelen hozzáférés elleni védelemről.

Továbbá:

- felelős a Társaság informatikai rendszer hardver eszközeinek karbantartásáért,
- gondoskodik a folyamatos vírusvédelemről, a vírusfertőzés gyanúja esetén intézkedik a fertőzött rendszerek vírusmentesítéséről (informatikus értesítése),
- ellenőrzi a védelmi eszközökkel való ellátottságot,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

Az adatvédelmi felelős nyilvántartást vezet:

- a beszerzett, illetve üzemeltetett hardver és szoftver eszközökről,
- a szerverhez, VPN hálózathoz, e-mailrendszerhez, munkaállomásokhoz tartozó hozzáférési adatokról,
- a Társaság által üzemeltetett honlapok elérhetőségéről, valamint a holnapszerkesztésre jogosultakról,
- az irodaház riasztórendszeréhez kiadott kódokról.

Az adatvédelmi felelős az adatkezelés törvényességének biztosítása érdekében köteles:

- ellenőrizni a jelen szabályzatban foglalt rendelkezések betartását;
- kezdeményezni a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) felé az Info. törvényben meghatározott nyilvántartásba vételi eljárás lefolytatását
- az ügyvezetés által meghatározott időpontig (pl január 15.) jelentést készíteni az ügyvezető részére a társaság adatvédelmi feladatainak végrehajtásáról
- évente legalább egy alkalommal teljes körű ellenőrzést végezni, amelynek tapasztalatairól tájékoztatja az ügyvezetőt;
- részt venni minden olyan szabályozás, módszertani eljárás előkészítésében, kidolgozásában, valamint minden olyan tanácskozáson, amelyek a védelem alatt álló adatokat, szabályozásukra vonatkozó rendelkezéseket érintik;

- az észlelt hiányosságokra és jogellenes magatartásokra köteles az ügyvezető igazgató figyelmét felhívni;
- ellenőrizni a szoftverek használatának jogszerűségét,
- ellenőrizni a védelmi előírások betartását.

7.2. Rendszergazda feladatai (megbízás alapján, külső vállalkozó végzi)

A rendszergazda a saját feladatkörébe tartozó rendszert felügyeli:

- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását.

7.3. A cégvezető, mint informatikai vezető feladatai és jogai

- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- előzetes bejelentési kötelezettség nélkül ellenőrizheti az informatikai munkafolyamat bármely részét,
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet,
- jogosult bármely érintett szervezeti egységnél ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos.

8. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy a megelőző intézkedésekkel felkészülten a veszélyhelyzetek elháríthatók legyenek.

8.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás (földrengés, árvíz, tűz, villámcsapás, stb.),
- környezeti kár (légszennyezettség, nagy teljesítményű elektromágneses térerő, elektrosztatikus feltöltődés, a levegő nedvességtartalmának felszökése vagy leesése, piszkolódás, pl. por),
- a közüzemi szolgáltatásban bekövetkező zavarok (feszültség-kimaradás, feszültségingadozás, elektromos zárlat, csőtörés).

8.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,

- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

Figyelem: a szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyeztetheti a feldolgozás folyamatát, és alkalmat adhat az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

9. Általános rendészeti védelem

Az informatikai eszközöket csak a Társaság alkalmazottai, vagy az arra felhatalmazott személyek (pl. gyakornokok) használhatják. Az eszközök rendeltetésszerű használatáért a felhasználók felelősek.
A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik. Az alapgép megbontását (kivéve a garanciális gépeket) csak az informatikus végezheti el.
A munkaidő lejártát követően az adott irodát utoljára elhagyó munkatárs köteles ellenőrizni, hogy minden számítástechnikai eszközt áramtalanítottak-e. Ez alól kivételt képeznek a központi számítógépek (szerverek) és azok szünetmentes üzemelését biztosító eszközök.
A felhasználó munkaviszonyának megszűnésekor minden informatikai eszközt a kiadáskor felvett nyilvántartás szerint, regisztrált módon vissza kell szolgáltatni a rajtuk tárolt, a Társaság tulajdonát képező adatokkal együtt, és ezzel egyidejűleg meg kell szüntetni a hozzáférési jogosultságait is.

10. Informatikai eszközök használata és az azokhoz kapcsolódó védelmi feladatok

10.1. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

A központi gépeket, szervereket a szünetmentes áramforrás megvédi a feszültségingadozásoktól, valamint áramkimaradás esetén az adatvesztéstől. A szerveren tárolt adatokról folyamatosan biztonsági mentést kell készíteni (minden este).
A Társaság minden felhasználó számára biztosítja a munka elvégzéséhez szükséges informatikai eszközöket. A számítógép munkaeszköz, átvétele után minden felhasználó köteles felelni annak épségéért a hardver és a szoftver tekintetében egyaránt.

A számítógépek bekapcsolását jelszóval vagy más azonosítóval védeni kell. Az adott eszközhöz tartozó jelszavakat az eszköz használatára jogosultakon és az adatvédelmi felelősön kívül csupán a karbantartást, javítást végzők ismerhetik meg. A mindenkori érvényes jelszavak listája és hozzáférhetősége az adatvédelmi felelősnél található.
A számítástechnikai berendezések elhelyezését a Társaság irodái között megváltoztatni csak az ügyvezető előzetes jóváhagyásával lehet.
Amennyiben azt a felhasználó munkája szükségessé teszi, a Társaság hordozható számítógépet biztosít részére. A notebook hordozhatósága miatt a rajta tárolt adatok igen veszélyeztetettek, ezért ezeket megkülönböztetett figyelemmel kell kezelni, hogy ne kerülhessenek illetéktelen kezekbe. A hordozható számítástechnikai eszközökre vonatkozó további előírások:

- Az egyénnek lehetőség szerint magánál kell tartani a gép márkáját, típusszámát és sorozatszámát a hordozható számítástechnikai eszköztől és tartótáskájától elkülönítve, úgy, hogy elveszítés esetén pontos információ álljon rendelkezésre.
- A hordozható számítógépes eszköz elveszítését/ellopását jelenteni kell a rendőrségnek, az ügyvezető igazgatónak valamint az adatvédelmi felelősnek az elvesztéstől/ellopástól számított 24 órán belül. Ha a munkatárs nem fordított kellő gondot a hordozható-számítástechnikai eszköz őrzésére, felelőssé tehető a csere költségének erejéig.
- A hordozható számítástechnikai eszközön tárolt adat biztonsági mentése a felhasználó kötelessége.

A számítástechnikai berendezésekről az adatvédelmi felelős köteles pontos, valamennyi változást naprakészen követő kimutatást vezetni, amely tartalmazza a berendezés:

- megnevezését,
- a használó, azért felelősséget vállaló nevét,
- az eszköz leltári számát.

Az informatikai és audiovizuális berendezéseket a Társaságtól bármely célból (otthoni munkavégzés engedélyezése, kiküldetés, rendezvények) csak az ügyvezető írásbeli vagy szóbeli engedélye alapján, az adatvédelmi felelős egyidejű tájékoztatásával lehet kivinni. Külsős cég részére történő átadást átadás-átvételi jegyzőkönyvben kell rögzíteni.
Az átadás-átvételi bejegyzésben fel kell tüntetni:

- a berendezés pontos megnevezését, azonosítóját (leltári számát)
- az átvevő pontos megnevezését,
- az átadás helyét, idejét, célját, indokát,
- a berendezés visszaszolgáltatásának várható időpontját
- a berendezés visszavételezésének dátumát.

A felhasználó az általa használt számítástechnikai eszközök felépítését, konfigurációját (pl. alkatrészek cseréje, hozzáadása, átkábelezés) nem módosíthatja. Az irodatechnikai, számítástechnikai berendezések bárminemű üzemzavara, illetve meghibásodása esetén a munkatársak haladéktalanul kötelesek értesíteni az adatvédelmi felelőst, aki gondoskodik az eszköz javíttatásról. Az eszközöket a Társaság telephelyeiről - kivéve, ha erre az ügyvezető igazgató külön engedélyt ad - csak az ő tudtával szabad kivinni, külső cég részére átadni javítás céljából. Az irodatechnikai, számítástechnikai berendezések karbantartását és javítását a megbízási szerződés alapján külső cégek végezhetik, vagy az ügyvezető igazgató előzetes engedélyével eseti javítás vehető igénybe más szolgáltatótól. A karbantartást, javítást végző külső cégekkel a tevékenység kapcsán tudomására jutott adatokkal kapcsolatosan titoktartási nyilatkozat aláírása kötelező. A karbantartást, javítást végző megbízási tevékenységgel rendelkező cégek szerződéseit rendszeresen felül kell vizsgálni.

Nem a Társaság kezelésében lévő számítástechnikai eszközzel az internet hálózat használható. A belső hálózathoz, szerverhez való hozzáférés az ügyvezető igazgató engedélyével lehetséges.

11. Szolgáltatások, alkalmazások igénybe vétele

11.1. Alkalmazások használata, védelme

Számítógépre telepítendő szoftverek, és a reális, a felhasználó munkakörének megfelelő jogosultsági szint igénylése a felhasználó a feladata. A jogosultságokat az ügyvezető igazgató engedélyezi az adatvédelmi felelős előterjesztése alapján, úgy, hogy a felhasználó csak a munkájához szükséges adatokhoz férjen hozzá.
A szerzői jog által védett számítógépes szoftverek bármilyen illegális, a jogtulajdonos engedélye nélküli használata, másolása törvénybe ütköző cselekedet, és mint ilyen határozottan ellenkezik a Balatoni Integrációs Kft politikájával. Ezért a Társaság használatában lévő, bárhol üzemeltetett számítógépeken csak olyan engedélyezett, jogtiszta szoftvereket szabad használni, amelyeket a Társaság bocsát a felhasználók rendelkezésére.
Tilos a cég tulajdonában álló számítógépekre, hálózatokra illegális szoftvert telepíteni! Az illegálisan telepített szoftvereket a számítógépről és a hálózatról azonnal törölni kell. Erről a felhasználót, valamint a Társaság ügyvezetőjét értesíteni kell.
A számítógépre történő szoftvertelepítést csak az adott alkalmazás rendszergazdája, vagy az ezzel megbízott informatikai munkatárs végezheti el. A felhasználók gépükre más szoftvereket önállóan nem telepíthetnek, nem másolhatnak.
A Társaság által vásárolt felhasználási-, vagy tulajdonjoggal rendelkező szoftverek a cég vagyonát képezik, ezért tilos ezeket külső személy vagy társaság részére átadni, másolni, vagy hozzáférhetővé tenni – beleértve a hálózaton vagy Interneten való hozzáférés lehetőségét is – kivéve, ha erről a szerződések másként rendelkeznek.
Gondoskodni kell arról, hogy az időtartamhoz kötött licencek időben legyenek meghosszabbítva.
A szoftver környezetre vonatkozó védelem kiterjed:

- a vásárolt, bérelt, fejlesztetett vagy saját fejlesztésű szoftver védelmének,
- az adatállományok szoftver eszközökkel történő védelmének,
- az adatállományok illetéktelen szoftver alkalmazásától való védelmének biztosítására.

Új szoftverek beszerzését, programok fejlesztetését, csak az adatvédelmi felelős és az informatikai munkatárs – esetenként megbízott belső vagy külső munkatárs - végezhetik, kivéve, ha a szerződés vagy a szoftverre vonatkozó szabályok másként nem rendelkeznek. Továbbá kötelesek ellenőrizni, illetve a szükséges intézkedéseket megtenni annak érdekében, hogy a szoftverek a számítógépek működőképességét ne sértsék, illetve az adatállományok sérülését megakadályozzák.
Az adatvédelmi felelős és az informatikai munkatárs együttműködve felelős és köteles gondoskodni:

- a szoftverek rendeltetés- és szabályszerű üzemeltetéséről,
- a szoftvernyilvántartás vezetéséről,
- a programdokumentációk őrzéséről, karbantartásáról,
- az esetleges változások elkészíttetéséről, átvezetéséről,
- az üzemeltetés hibáinak kiküszöbölése érdekében szükséges intézkedések megtételéről, valamint
- az illetéktelen hozzáférés megakadályozásáról, az illetéktelen próbálkozás kizárásáról.

A Társaság informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
A Balatoni Integrációs Kft. hálózati és számítógépes erőforrásainak személyes használata megengedett, ha az ilyen használat eseti és jelentéktelen, és nem zavarja a normál munkatevékenységet. A személyes használat:

- nem kötődhet ügynöki tevékenységhez, hacsak nem kaptak rá írásos engedélyt;
- nem lehet semmilyen politikai szervezettel kapcsolatos, kivéve, ha ettől eltérő megegyezés született;
- nem reklámozhat haszon ellenében semmit, ami kívül esik az üzleti tevékenységen és
- nem okozhat semmilyen kellemetlenséget és nem kérdőjelezheti meg a Balaton Fejlesztési Tanács és a Balatoni integrációs Kft. jó hírét.

Tilos a Társaság hálózati és számítógépes erőforrásainak használata a következő célokra:

- személyes haszonszerzés,
- személyes üzleti tevékenység,
- személyes politikai célok,
- társadalomellenes vagy etikátlan viselkedés,
- olyan tevékenységek, melyek sértik a nemzetközi, országos, szövetségi, állami vagy helyi törvényeket vagy előírásokat,
- lánclevelek küldése/továbbküldése,
- játékprogramok futtatása munkaidőben (még az operációs rendszerhez mellékelteket is szigorúan tilos),
- a bizalmas információk jogosulatlan felfedése, továbbítása,
- bármely hálózati vagy számítógépes erőforráshoz való jogosulatlan hozzáférés.

11.2. Hozzáférési jogosultság, jelszavak kezelése

Az adatok kezelésével, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátásával megbízott munkatársak az adatokhoz a feladatuk ellátásához szükséges mértékben férhetnek hozzá, azonban az adatokat nem használhatják fel más célra, és nem hozhatják mások tudomására.
A felhasználók az alkalmazásokhoz, szolgáltatásokhoz való hozzáférés kiadásakor felhasználó-azonosítót és jelszót kapnak. A kapott jelszót a felhasználó köteles titokban tartani, nyilvánosságra kerülés gyanúja esetén azonnal azt meg kell változtatnia.
Javasolt, hogy a jelszó ne legyen könnyen kitalálható, kikövetkeztethető (pl. ne értelmes szó legyen, legyen benne szám, kis és nagybetű vegyesen stb.), valamint azt szükség szerint a felhasználó köteles időközönként megváltoztatni
Más felhasználó hozzáférési jogosultságával (jelszavával) való visszaélés, az engedélyezett jogosultságtól eltérő használat kísérlete fegyelmi vétség, amelynek a súlyosság mértékétől függően büntetőjogi következményei is lehetnek.
A számítástechnikai alkalmazások esetén a hozzáférést biztosító jelszavakat az adatvédelmi felelős zárt borítékban biztonságosan tárolja. A jelszavakat tartalmazó boríték szükség szerinti felbontásáról - az adatvédelmi felelős távollétében - a bontást végző köteles jegyzőkönyvet készíteni.
A bejelentkezés után a hálózati és számítástechnikai eszközöket nem szabad felügyelet nélkül hagyni, amikor a cég hálózatához vannak kapcsolódva.
Az adatkezelő köteles az illetéktelen adatkérő, illetve igénylő részére az adathozzáférés és felhasználás minden formáját megtagadni. Minden olyan eseményről, melynek során jogtalan adatkezelésre kérték fel vagy utasították, illetve ha jogellenes adatkezelést észlelt, köteles az adatvédelmi felelős mellett a Társaság ügyvezetőjét is haladéktalanul tájékoztatni.

A Társaság minden alkalmazottja, vállalkozója, szakértője és partnere felelős az elektronikus információknak a megőrzéséért (jogosulatlan hozzáférés, információ illetéktelen megváltoztatása, vagy elpusztítása).

11.3. Levelezési rendszer használata

A Balatoni Integrációs Kft-nél elektronikus levelezés céljára az Outlook valamint a Mozilla Thunderbird rendszer üzemeltethető.
Valamennyi felhasználó, akinek a munkájához ez szükséges, rendelkezik elektronikus postaládával, amihez felhasználónév és jelszó tartozik, amelyet a felhasználó a Társasághoz való belépéskor kap meg. Az e-mail rendszerhez való hozzáférésekről az adatvédelmi felelős nyilvántartást vezet. Minden felhasználó megtalálható a belső levelezőrendszer címlistájában.
A céges e-mail címre külső (Internet) elektronikus levelek is fogadhatóak, illetve küldhetők. A levelek tartalmáért minden esetben a postafiók tulajdonosa felel. A céges e-mail címmel küldött tartalom, hozzászólás, véleménynyilvánítás a Társaság nevében történő hivatalos nyilatkozatnak minősül, azért a felhasználó felelősséggel tartozik.
A felhasználó tudomásul veszi és elfogadja (Felhasználói nyilatkozaton aláírásával igazolja a tudomásulvétel tényét), hogy a Balatoni Integrációs Kft ügyvezető igazgatójának minden céges e-mail-címre érkezett, és arról küldött levélbe betekintési joga van.
A Társaság biztosítja a levelező távoli elérését webmailen keresztül. A dolgozók felelőssége, hogy a nem a Társaság tulajdonában lévő számítógépen (dolgozó otthoni gépe, nyilvánosan elérhető munkaállomások) a felhasználók nem hagyhatnak céges adatokat:

- dokumentumok nem menthetők helyileg a PC merevlemezére.
- nyilvános munkaállomáson (internetes kávéház, szálloda PC-je) a webmail megtekintése a böngészőben privát ablakban történjen, vagy azonnal törölni kell az előzményekből.

11.4. Az Internet használata

Minden felhasználó, akinek a munkájához szükséges, jogosult az Internet, böngésző használatára.
A megfelelő sebességű szolgáltatás folyamatos biztosítása érdekében

- az internetszolgáltatókkal kötött szerződést rendszeresen felül kell vizsgálni
- a felhasználók számára kerülendő az egy munkaállomásról közel egy időben indított több, nagyobb méretű adatállomány letöltése, mivel ez jelentősen csökkenti a többi felhasználóra jutó adatátviteli kapacitást.

Mint minden, a Társaság eszközein tárolt adat, a megtekintett oldalak, illetve azok naplófájlja is a Társaság tulajdonát képezik, amennyiben erről a szerzői jogok másképp nem rendelkeznek. Az ügyvezető igazgatónak az Internet használat során képződő naplófájlokba betekintési joga van, azokról a Társaság által megbízott informatikus az ügyvezető igazgató kérésére adatot szolgáltathat.
Tilos az Internet használata a Társaság hálózati vagy számítógépes erőforrásokkal játékok játszására, vagy a cég hitvallásával ellentétes anyagok megszerzésére, terjesztésére, úgymint faji, vallási, hitbeli, nemi értelemben sértő vagy pornográf, illetve szexuális irányultságú anyagok.
A Balatoni Integrációs Kft. fenntartja a jogot arra, hogy megszűrje, illetve korlátozza a Társaság internet kapcsolatán keresztül elérhető tartalmat.
Nem javasolt az Internetről a munkához nem szükséges állományok letöltése, oldalak böngészése, számítógépre való telepítése, mert azok instabillá tehetik az informatikai infrastruktúrát. Amennyiben bizonyítható, hogy ilyen tevékenység következtében sérül a hálózat, a keletkezett kárért a felhasználó felel. A nem megfelelő használat esetén a hálózatban a hozzáférés korlátozható, illetve megvonható.

11.5. Weboldalak

A szerverek, weboldalak folyamatos működését, elérhetőségét és biztonsági monitorozását. megbízott külső informatikai cég biztosítja.
Minden munkatárs előzetes egyeztetéssel szakterületén belül kérheti információ, dokumentum feltöltését, törlését, áthelyezését és a technikailag problémás dokumentumok konvertálását a társaság honlapjára.
Minden szervezeti egység

- jogosult a honlap szerkesztőségi rendszeréhez egy kijelölt munkatársán vagy a honlapra szerkesztésre kijelölt munkatárson keresztül hozzáférni vagy a honlapot szerkeszteni,
- köteles a honlap illetékességből hozzá tartozó menüpontjainak naprakészen tartásáról gondoskodni, az elavult, lejárt dokumentumokat törölni vagy archívumba helyezni.

Az adatvédelmi felelős tartja nyilván a Társaság által üzemeltetett honlapokat valamint a honlap szerkesztésével megbízott munkatársak hozzáférési jogosultságát.

11.5. VPN hálózat használata

Virtuális magánhálózat, mely a távoli gépek részére biztonságos saját hozzáférést biztosít a hálózathoz.
A VPN hálózat sebességet az Internet vonal kapacitása, a feltöltés sebessége határozza meg. A folyamatos távmunka nem ajánlott, mivel az internetet lassíthatja azt.
A VPN hálózathoz való csatlakozás az adatvédelmi felelőstől igényelhető, aki a korábban kiadott igényeket is köteles nyilvántartani. Amennyiben az ügyvezető igazgató engedélyezi az igénylő számára a szerver távoli elérését, a rendszergazda feladata kiadni a jelszót és elvégezni a szükséges beállításokat.

12. Adatbiztonság, adathordozók

12.1. Adatok kezelése, tárolása, adatállományok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.
Minden felhasználó a sikeres bejelentkezés után jogosultságának megfelelően férhet hozzá a szerveren tárolt munkakönyvtárakhoz.
A Társaság kizárólag a hálózati meghajtókon tárolt adatok biztonságáért vállal felelősséget, a lokális meghajtókon, és hordozható adathordozókon tárolt adatok biztonságáért, bizalmasságáért a felhasználó tartozik felelősséggel. Emiatt általában is, de a cég számára fontos állományok esetében különösen javasolt a hálózati meghajtók (Központi szerver – Siófok, pénzügyi szerver - Siófok, NAS szerver - Balatonfüred) használata a biztonságos ügyintézés érdekében.
A felhasználók a munkahelyi tevékenységükkel kapcsolatosan keletkezett adatokat a hálózati szervereken a számukra vagy az adott faladat számára kijelölt könyvtárakban helyezhetik el. Ez a tárterület csak e tevékenységekkel kapcsolatos adatok tárolására ajánlott. A könyvtárak hozzáférési jogosultsági rendszerének beállítása az adatfelelős és a rendszergazda közös feladata.
A könyvtárak elnevezésének egyértelműen utalnia kell a benne elhelyezett tartalomra. A területek adattartalmáért a jogosult felhasználók felelnek.

Mivel a központi szerveren tárolt adatok rendszeresen (naponta) mentésre kerülnek, probléma (adatvesztés) esetén általában az előző nap mentett állapota állítható vissza.
A hálózati meghajtók a Társaság számára is információval bíró adatok tárolására szolgálnak, azokon privát adatok, képek tárolása csak időszakosan lehetséges, hosszú távon nem engedélyezett.
A szerveren tárolt, nem közérdekű (különösen: magánjellegű) vagy az aktualitásukat veszített közérdekű tartalmakat (különösen: videók, fényképek, és más hasonló jellegű adatállományok), amennyiben a munkavégzést akadályozzák a tulajdonos értesítését követő 24 óra elteltével törölhető.
A központilag mentett állományok visszatöltésére az adatvédelmi felelős és az informatikai munkatárs jogosult. A helyi mentés adatállományainak visszatöltésére az egyes alkalmazásokért felelős munkatárs a jogosult. Ezeket az állományokat, valamint a kívülről érkező adatokat a vírusfertőzés kizárása érdekében előzetesen tesztelni, szükség esetén vírus-mentesíteni kell, amely az adott alkalmazásért felelős munkatárs feladata.
Az adatok védelme az adathordozó fajtájától független. A rendszerből papírra kinyomtatott, fájlba exportált adatokhoz való hozzáférés szintje meg kell egyezzen a rendszerbeli hozzáférés szintjével. Valamely rendszerhez jelszavas hozzáféréssel rendelkező felhasználó a rendszerből nyomtatott adatokat, exportált fájlokat nem tarthatja, tárolhatja hozzáféréssel nem rendelkező felhasználók által elérhető helyen.
Az adatszolgáltatást igénybe vevő, az általa észlelt adathiba esetén, erről a hozzáférési jogosultsággal felhatalmazott munkatársat köteles értesíteni, aki köteles a javítás elvégzéséről intézkedni.
Kilépő felhasználó és ideiglenesen a cégnél dolgozó külső szakértő távozása esetén az általa használt és tárolt adatok fontosak lehetnek az adott területen tovább dolgozó számára. A távozó személy adatainak kezeléséért, azok további elhelyezéséért a felhasználó felettese, illetve külső szakértő esetén a szerződéskötő vagy kapcsolattartó a felelős.
Az egyes alkalmazásokat futtató munkatársak kötelesek gondoskodni arról, hogy a tárolt programok ne károsodjanak, továbbá a rendszertervben rögzített követelményeknek megfelelően működjenek.
Módosított, illetve új programot csak tesztelést követően lehet üzemszerűen használatra átvenni, miután bebizonyosodott, hogy a tesztelés alatt az a feladatnak megfelelően és hiba nélkül működött, valamint adatvesztés vagy sérülés nem történt.
Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

12.3. Hangfelvétel védelme

Minden olyan hangfelvétel, ami a Társaság működése során a személyes adatok védelméről, valamint az államtitokról és a szolgálati titokról szóló jogszabályok alapján védett, illetve minősített adatot tartalmaz, a jelen utasításban meghatározott védelemben részesül.
A Balaton Fejlesztési Tanács és Bizottságai üléseiről valamint egyéb, a szó szerinti jegyzőkönyvet elváró eseményekről készített hangfelvételeket csak az adott testület, szervezet tagjai, hivatalos (az esemény kapcsán ellenőrző, megbízó hatállyal rendelkező) szervezetek, az arról hivatalos, írásos jegyzőkönyvet készítők valamint egyedi engedéllyel rendelkezők hallgathatják vissza a Társaság hivatalos helyiségében.
A Tanács és bizottságainak üléseiről készített hangfelvételeket egy hónap elteltével lehet selejtezni. Az egyéb hangfelvételeket a mindenkori elvárt időtartamig kell megőrizni.

A hangfelvételeket az Társaság hivatalos helyiségeiből kivinni tilos, kivételt képeznek ez alól a hivatalos (az esemény kapcsán ellenőrző, megbízó hatállyal rendelkező) szervezetek ez irányú kérelme.
Az Társaságnál folytatott egyéb, belső, zártkörű tárgyalásokról, megbeszélésekről készített hangfelvételek őrzésére, a hozzáférési jogosultságra vonatkozó szabályokat az ügyvezető igazgató határozza meg azonban ezek tárolási és feldolgozási szabályai alapvetően megegyeznek az egyéb hangfelvételeknél megfogalmazottakkal.

13. Számítógépes kártevők elleni védelem – Vírusvédelem

Számítógépes kártevők nem hasznos tevékenységet folytató programok, melynek sokféle fajtája létezik: vírusok, férgek, trójai programok, kémprogramok, egyéb káros program, és tevékenységek. (Bővebben: 3. Az adatkezelés során használt fontosabb fogalmak)

13.1. Kártevők felismerése

Kártevőkre gyanakodhatunk, ha:

- lelassul a számítógép működése, gyakran percekig csak tölt, és ez alatt semmilyen funkció nem érhető el.
- egy funkció nem úgy működik, ahogy megszoktuk, vagy megváltoznak a program beállítások.
- hardverhibával nem megmagyarázható adatvesztés történik.
- az internetes kommunikáció lelassul.

13.2. Védekezési módszerek

Vírusirtók használata
A vírusirtó program képes felismerni, és a legtöbb esetben eltávolítani a fertőzött gépről a vírust. Figyelni kell arra, hogy a programot naponta kell frissíteni, hogy felismerje a legújabb vírusokat is. Az ingyenesen elérhető vírusirtók közül az AVG Free, vagy az Avast Home ajánlható, a fizetősek közül például a NOD32, a Kaspersky Antivirus, vagy a Norton Antivírus.
Kém és trójai program irtók
Hasonlóak a vírusirtókhoz, csak ezek trójai és spyware programokat keresnek és irtanak a gépünkön.
Tűzfalak
A tűzfal feladata megvédeni a mögötte lévő gépeket a kívülről (pl. internet) jövő veszélyekkel (betörési kísérlet, ártó programok) szemben, illetve ellenőrzik a bonyolított hálózati forgalmat.
Egyéb, de fontos tevékenységek:

- adatmentés, arhiválás. Minden esetben készíteni kell a dokumentumainkról biztonsági másolatot.
- ismeretlen feladótól érkező levél megnyitás nélküli törlése, de legalább a csatolt állományok figyelmes kezelése.
- az operációs rendszer és a fontosabb programok rendszeres frissítése. Sokszor programhibát kihasználva terjednek a kártevők. Ezeket a hibákat a programok újabb verzióiban többnyire kijavítják, így kisebb az esély a károkozásra.
- csak jogtiszta programok használata. Gyakran a kémprogramokat, és a trójai programokat ingyen elérhető, de normál esetben fizetős programokba rejtve juttatják el a gépekre.

Az adatvédelmi felelős és az informatikai munkatárs köteles gondoskodni olyan szoftvertermékek beszerzéséről, amelyek biztosítják a vírusok kiszűrését, megsemmisítését, a vírus okozta károk helyreállítását.
A számítógépek hálózatra történő bejelentkezésekor a vírusellenőrző szoftver vírusminta állománya automatikusan frissül. A felhasználó minden esetben köteles a vírusírtó programot naprakészen tartani, az elmaradt frissítés következtében bekövetkező vírusfertőzés károkért a felhasználó a felelős.
A vírusirtó szoftver futása időnként a számítógép lassulását eredményezheti, azonban a szoftver eltávolítása, működésének megakadályozása semmilyen körülmények között nem engedélyezett. Az ebből eredő károkért a rendszer működését akadályozó felhasználó a felelős.
Vírusfertőzés gyanúja esetén a felhasználók az adatvédelmi felelőshöz és az informatikai munkatárshoz fordulhatnak.

14. Selejtezés, megsemmisítés

Az adatokat tartalmazó adathordozó megsemmisítésére, illetve törlésére csak az alkalmazás felelősének hozzájárulásával kerülhet sor.
A megsemmisítést az ezzel megbízott munkatárs, illetve az erre szerződés, megrendelés alapján megbízott végezheti, az adatvédelmi felelős, illetve az ügyvezető igazgató tájékoztatása és egyetértése mellett. A megsemmisítésről jegyzőkönyvet kell készíteni.
A feleslegessé, illetve használhatatlanná vált, a gazdaságosan már nem javítható számítástechnikai berendezések selejtezésére a Selejtezési szabályzat előírásait kell alkalmazni.

15. Adatvédelmi tájékoztató munkavállalók részére

Az érintettek (munkavállaló, volt munkavállaló) jogainak érvényesítése kapcsán az érintett a személyes adatai kezelésről tájékoztatást illetve törlést kérhet. A kérelmet írásban kell benyújtani. (Info tv. 13. bekezdés Az érintettek jogai és érvényesítésük)

15.1. Munkavállalók munkaviszonnyal összefüggő adatkezelése

A munkavállalók személyes adatai a Mt. szerinti adatkörben különös tekintettel a 2012. évi I. tv 10-11 §-ára kezelhetők.

Az adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása.

A kezelt adatok köre:

Munkavállaló kapcsán

- a neve,
- a születési neve,
- a születési helye és ideje,
- az állampolgársága,
- a törzsszáma,
- az anyja születési neve,
- a lakóhelyének címe,
- a tartózkodási helye (amennyiben eltérő a lakóhelytől),

- a magán-nyugdíjpénztári tagság ténye, belépés ideje (év, hó, nap), bank neve és kódja
- az adóazonosító jele,
- a társadalombiztosítási azonosító jele (TAJ szám),
- a nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
- a folyószámla száma,
- a munkaviszony kezdő napja,
- a biztosítási jogviszony típusa,
- a heti munkaórák száma,
- a telefonszáma,
- a családi állapota,
- a végzettséget igazoló okmány másolati példánya,
- a munka-alkalmassági egészségügyi igazolás,
- a munkaköre,
- az orvosi alkalmasság ténye,
- az erkölcsi bizonyítvány kiállításának dátuma, okmányszáma, kérelem azonosítója,
- a leszámolást követően a munkaköri alkalmassági záró orvosi vizsgálat elvégzésének ténye (amennyiben szükséges),
- meghatározott munkakörben a vezetési engedély kategóriánkénti egészségügyi alkalmasságának, lejártának időpontja,
- a főálláson kívüli munkavégzés esetén: jogviszony jellege, munkáltató neve és székhelye, a főálláson kívüli munkahelyen teljesített havi átlagos munkaidő, elvégzendő tevékenység,
- az Mt. 120. § alapján járó pótszabadság igénybevételével kapcsolatosan
    - a rehabilitációs szakértői szerv legalább ötven százalékos mértékű egészségkárosodását megállapítását igazoló okmány fénymásolata
    - a fogyatékossági támogatásra jogosultságot igazoló okmány fénymásolata,
    - a vakok személyi járadékára jogosultságot igazoló okmány fénymásolata,
- a pótszabadság, családi adókedvezmény igénybe vétele, adómentes természetbeni juttatásnak minősülő kedvezményes utazási igazolvány igénylésének vagy iskolakezdési támogatás céljából munkavállaló hozzátartozójának:
    - a születési helye és ideje,
    - a lakcíme,
    - az anyja neve
    - a társadalombiztosítási azonosító jele (TAJ szám)
    - az adóazonosító jele,
    - az érvényes diákigazolvány meglétének ténye.

Az adatkezelés jogalapja: törvényi felhatalmazás [a munka törvénykönyvéről szóló 2012. évi I. törvény 10. § (1) és (3)] és az érintett hozzájárulása [Infotv. 5 § (1) a) és 6. § (6)];

Az adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint

- a munkaviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig,
- a munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig

Az adatkezelés módja: elektronikus

15.2. Munkavállalók ellenőrzésével összefüggő adatkezelés

A munkáltató ellenőrizheti a munkavállalókat a munkaviszonyból eredő kötelezettségek teljesítése céljából a munkaviszonnyal összefüggő magatartása körében. Az ellenőrzésre a munka törvénykönyve [11. § (1)-(2)] ad jogalapot.
A társaságnál bizonyos beosztásokhoz céges telefont és e-mail címet kapnak a munkavállalók. Az irodai dolgozók számára a cég számítógépet is biztosít.
A Társaság tulajdonát képező személyi számítógépeket és laptopokat, mivel a céges e-mail címeket a Kft. munkavégzés céljából biztosítja, ezért a munkavállaló ezen eszközökön tárolt magáncélú személyes adatait (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) a Társaság a számítógép ellenőrzése során bármikor megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a Társasági eszközön való személyes adatok tárolása az adatkezeléshez történő 2011. évi CXII. törvény 5. § (1) a) szerinti érintetti hozzájárulásnak minősülnek.
Mindazon e-mail címek, amelyekben a Társaság neve kiterjesztésként benne foglaltatik, a Társaság tulajdonát képezik. Ezen címeken a Társaság munkavállalói által folytatott levelezés munkacélú levelezésnek minősül. Az ilyen címeken folytatott levelezésbe a Társaság megfelelő jogalap esetén jogosult betekinteni. A Társaság jogosult a fent nevezett címeken folytatott levelezések meghatározott időközönkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében adatbiztonsági okokból saját eszközein bármilyen állomány törlésére.
Amennyiben a munkavállaló e-mail címén található leveleiben magáncélú személyes adatait, kifejezett utalás nélkül tárolja, úgy a Társaság az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti.

A munkáltató jogosult ellenőrizni a munkahelyi postafiókot és internet használatot. Mindemellett főszabály szerint a magáncélú levelek tartalmát a munkáltató munkaviszonyból fakadó jogosultság érvényesítése során sem jogosult megismerni. Ellenőrzés esetén:

- **az adatkezelés célja**: a Társaság jogos üzleti érdekeinek megfelelően a munkavállalók Mt. 11. § (1)(2) bekezdése szerinti ellenőrzése, így különösen a munkavállalónak biztosított számítógép, e-mail cím, telefonhasználat és internet-hozzáférés ellenőrzése.
- **a kezelt adatok köre:** az ellenőrzés során rögzített személyes adatok, így különösen magán e-mail címek, magán telefonszámok, fényképek, saját számítógépes dokumentumok, internetes böngészési előzmények, cookie-k, munkajogviszony ellátása során észlelt jogsértés ténye, a jogsértés leírása.
- **az adatkezelés jogalapja:** 2012. évi I. törvény 11. § (1) (2) bekezdése és esetlegesen 2011. évi CXII. törvény 5. § (1) a)
- **az adattárolás határideje:** az ellenőrzéstől számított 1 év, de legkésőbb az ellenőrzéssel kapcsolatos igény elévülése.

16. Záró rendelkezések

Az Adatvédelmi Szabályzat és Informatikai Házirend kihirdetésekor lép hatályba.
Az Adatvédelmi Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.
A társaság adatkezelési eljárásával kapcsolatos panasszal a Nemzeti Adatvédelmi és Információhatóság Hatósághoz (NAIH) lehet fordulni. Cím: 1024 Budapest, Szilágyi Erzsébet fasor 22/C. (www.naih.hu)

A Társaság adatvédelmi felelőse a Kft. titkára.
2016. május 24-én az Európai Unió a személyes adatok védelme érdekében Általános Adatvédelmi Rendeletet – GDPR - tett közzé:
Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását, valamint a 95/46/EK rendelet hatályon kívül helyezését (általános adatvédelmi rendelet) szabályozza.
A szabályozásnak **2018. május 25-től** minden személyes adatokat kezelő szervezetnek meg kell felelnie, ezért a fenti szabályzat a rendeletnek megfelelően 2018 tavaszán aktualizálásra kerül, melybe beépítésre kerül a 2/2016. sz. Ügyvezető igazgatói utasítás: Adattovábbítást és megosztást szabályozó igazgatói utasítás.

1. sz. melléklet

Felhasználói nyilatkozat

Alulírott, mint nyilatkozattévő aláírásommal igazolom, hogy a jelen Adatvédelmi Szabályzat és Informatikai Házirend előírásait megismertem, megértettem, tudomásul veszem és magamra nézve kötelezőnek tartom a Balatoni Integrációs Kft. informatikai eszközeinek használata során.

Nyilatkozattévő	Törzsszám	Nyilatkozattétel dátuma	Aláírás
Dr. Molnár Gábor	002		
Dr. Könczölné Egerszegi Zita	003		
Fekete-Páris Judit	004		
Györkéné Biczó Judit	005		
Majoros Attiláné	006		
Magyarfalvi Attila	0010		
Tóthné Bartos Éva	0011		
Bardóczy Árpád	0012		
Sárdi Enikő	0013		
Péterffy Ilona	0014		
Hegedűs István	0015		
Baliné Berlinger Ildikó	0016		
Oláh Miklós	0017		
Kulics Bea	0018		
Csákváriné Joó Zsuzsanna	0019		
Dombi Gábor	0020		
Kuborczik Barbara	0021		
Fekete Károly	0022		
Dr. Horváthné Labát Márta	0023		

Nyilatkozattévő	Törzsszám	Nyilatkozattétel dátuma	Aláírás
Lukács Zsófia Mária	0027		

2. sz. melléklet

Titoktartási nyilatkozat

Jelen nyilatkozatunkban megerősítjük abbeli megállapodásunkat és egyetértésünket, miszerint a Balatoni Integrációs Közhasznú Nonprofit KFT . által ..... *(név)* (..... - *anyja neve, születési hely és idő*) előtt az eddigiekben feltárt és a jövőben feltárandó bizonyos információk, így különösen üzleti tervek, kereskedelmi titkok, ügyfelek adatai és egyéb tulajdonosi információk, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény hatálya alá tartozó személyes adatok (összefoglalóan: információk) bizalmas jellegűek.

..... a nyilatkozat aláírásával elfogadja, hogy az ilyen információk egyetlen részét vagy töredékét sem teszi közzé, nem bocsátja rendelkezésre, vagy nem tárja fel más módon semmilyen harmadik fél előtt a **Kft.** ügyvezetőjének erre felhatalmazó előzetes írásbeli beleegyezése nélkül, kivéve, ha ezek az információk bizonyító erejű dokumentumokként nyilvánosságra bocsáthatók. Az ilyen információk nem tekintendők nyilvánosságra bocsáthatónak pusztán azért, mert ezekből további általános információkat lehet szerezni, vagy mert begyűjthetők egy vagy több forrásból is, vagy ha abból adódóan kerültek nyilvánosságra, mert megszegték a jelen nyilatkozatot, vagy harmadik személlyel vagy jogi személlyel kötött hasonló nyilatkozatokat.

Nyilatkozattevő beleegyezését adja, hogy mindent és minden ésszerű elővigyázatossági intézkedést megtesz annak érdekében, hogy szóban, írásos anyagban, vagy elektronikus adattároló eszközben vagy más módon feltárt ilyen információkat megfelelő védelemmel látja el bármely harmadik fél előtti jogosulatlan feltárással szemben, így különösen betartja a **Kft.** Adatvédelmi és adatbiztonsági szabályzatának irányadó rendelkezéseit. Beleegyezését adja ahhoz is, hogy egyetlen anyagról sem készít másolatot és az ilyen anyagok valamennyi másolatát kérésre azonnal visszaszolgáltatja.

Nyilatkozattevő elfogadja továbbá, hogy valamennyi ilyen információ tulajdonosa a **Kft.,** és hogy a **Társaság** folyamatos üzletvezetése érdekében mindezen információk bizalmas jellegűek, értékesek és nélkülözhetetlenek. Beleegyezését adja, hogy az ilyen információkat nem fogja felhasználni, kiaknázni és/vagy üzleti alapokra helyezni saját javára vagy bármely egyéb harmadik fél javára.

Jelen nyilatkozat aláírása nevezettet nem ruházza fel semmiféle jogosultsággal vagy egyéb joggal.

Jelen titoktartási nyilatkozat ..... (dátum vagy konkrétan meghatározható esemény, így pl.: „munkaszerződés aláírásával") lép életbe.

Jelen titoktartási nyilatkozaton megadott, a 2011. évi CXII. törvény hatálya alá tartozó személyes adatot a **Kft.** Adatvédelmi és adatbiztonsági szabályzata alapján kezeli.

....., 20.....

Nyilatkozattevő	Balatoni Integrációs Kft képviseletében