



Rest  
& Providence

## **INFORMATIKAI SZABÁLYZAT**

Nyilvántartásba vette a Fővárosi Törvényszék Cégbírósága 01-09-868949 cégjegyzékszámom

Székhelye: 1036 Budapest, Galagonya u. 5. 1. em

Honlap: <http://www.restandprovidence.hu>

## 1. A TÁRSASÁG TEVÉKENYSÉGE

A Társaság főtevékenysége a TEÁOR'08 szerint:

6831 Ingatlanügynöki tevékenység, további tevékenységek:

6832 Ingatlankezelés

7021 PR, kommunikáció

7312 Médiareklám

7320 Piac-, közvélemény-kutatás

## 2. A SZABÁLYZAT CÉLJA

A társaságnak szabályoznia kell a szolgáltatási tevékenység ellátásához alkalmazott informatikai rendszerét, rögzítenie kell annak védelmével, biztonságával kapcsolatos alapvető elemeket.

A Társaság munkavállalóinak száma két fő, a fentiek szerinti tevékenységvégzés kapcsán ügyfeleinek száma 250 alatt van.

A Társaság tevékenységének végzése során olyan informatikai rendszert használ, mely alkalmas arra, hogy a társaság munkatársai napi tevékenységüket problémamentesen végezzék, egymással és a társaság külső kapcsolataival megfelelőképpen kommunikáljanak, az adatkezelés és feldolgozás biztonságos módon történik, amely megakadályozza az informatikai rendszerhez a jogosulatlan hozzáférést, az észrevétlen módosítást. A Társaság gondoskodik az informatikai rendszer kockázatokkal arányos védelméről.

Jelen szabályzat – a Társaság működési feltételeit biztosító egyéb szabályzatokkal együttesen és összhangban - biztosítja:

- a titok-, vagyon- és tűzvédelmi előírások betartását,
- személyiségi jogok védelmét,
- a számítástechnikai eszközök rendeltetésszerű használatát és megfelelő üzemvitelét,
- a társaság szolgáltatását támogató műszaki fenntartási és karbantartási teendők elvégzését,
- esetleges illetéktelen hozzáférésből és felhasználásból eredő károk megelőzését, illetve minimális mértékűre való csökkentését,
- az adatállományok formai és tartalmi helyességének és épségének megőrzését,
- az alkalmazott szoftverek sértetlenségének, megbízható működésének biztosítását,
- az adatállományok biztonságos mentését,
- a felhasznált és keletkezett írásos dokumentumok megfelelő kezelésének biztosítását,
- a jogosultság és a hozzáférés rendszerének kialakítását.

**Jelen szabályzaton kívül mindezen fentiekkel összefüggésben a társaság a következő szabályzatot alkalmazza:**

- Adatkezelési szabályzat

### **3. A SZABÁLYZAT FELÜLVIZSGÁLATÁNAK RENDJE**

A szabályzat felülvizsgálatát két évente szükséges elvégezni. Amennyiben a társaság működési rendjében olyan változás történik, mely az informatikai rendszerre, annak biztonságára hatással van, úgy a felülvizsgálatot „soron kívül” el kell végezni és a szükséges változtatásokat át kell vezetni. A vonatkozó döntéseket a társaság bármelyik Ügyvezető Igazgatója önállóan meghozhatja.

A felülvizsgálatot a vonatkozó jogszabályok változása esetén is szükséges elvégezni és szükség esetén a változásokat átvezetni. A döntéseket az Igazgatóság hozza meg.

A szabályzatot és módosításait a tulajdonos hagyja jóvá.

### **4. A TÁRSASÁG INFORMATIKAI RENDSZERE**

A számítógépes hálózat a 1036 Budapest, Galagonya u. 5. I. emeleti irodahelyiségében üzemel, melyen keresztül a társaság adminisztrációja, ügyvitele, levelezése történik.

A társaság használatában van a MINI CRM vállalatirányítási rendszer, amely a cég tevékenységét hivatott racionalizálni, továbbá az adatok biztonságos kezelését szolgálja.

A számítógépes infrastruktúra teljes körű szoftveres és hardveres karbantartását szolgáltatási szerződés alapján külső társaság (továbbiakban: szolgáltató) végzi. A szolgáltató munkanapokon 9-17 óráig telefonos rendelkezésre állást biztosít. A kritikus problémák megoldását 48 órán belül megkezdi. Biztosítja a szoftveres tanácsadást, a szoftveres problémák szakmai támogatását. Amennyiben a társaság új hardver, vagy új szoftverek telepítése mellett dönt, azok telepítését elvégzi.

A MINI CRM rendszerrel kapcsolatos informatikai teendőket a rendszer szolgáltatója, karbantartója végzi.

A Társaság informatikai hálózata lehetőséget biztosít az egyéni és a csoportos munkára azzal, hogy:

- kommunikációs kapcsolatot teremt a házon belül, illetve a külvilág felé,
- közös információforrást biztosít, közös, illetve egységes információs bázist nyújt a munkatársak számára,
- a közös hálózati “erőforrások” minden hálózati munkahelyről elérhetővé teszik speciális eszközök használatát (pl. a CD lemezekben tárolt információk, lézernyomtató, stb.)
- a döntéshozók számára széleskörű, megbízható, aktuális adatok elérését teszi lehetővé.

A szabályozás fő alapelvei:

- minden felhasználó számára biztosítani kell a feladatai ellátásához szükséges és elégséges jogokat,
- szolgálnia szükséges az információk maximális védelmét,
- tegye lehetővé a biztonságos, ellenőrizhető működést,
- tisztázza a hálózat használatával és üzemeltetésével kapcsolatos jogokat és kötelezettségeket.

## **5. A SZABÁLYZAT TARTALMA**

A szabályzatban foglaltak a Társaság minden munkatársára vonatkoznak.

A szabályzatban foglaltaktól való eltérés esetén felmerülő problémák megoldására a szolgáltató nem kötelezhető, az elhárítás minden következménye és költsége a felhasználót terheli.

Ennek fokozatai:

- felhasználás korlátozása,
- kizárás a felhasználásból,
- fegyelmi eljárás kezdeményezése,
- büntető feljelentés tétele,
- kártérítési eljárás kezdeményezése.

## **6. FELHASZNÁLÓKRA VONATKOZÓ SZABÁLYOK**

A munkaállomást a felhasználó az alap operációs rendszer és az alap felhasználói szoftverek installálásával kapja meg.

A felhasználók a számítógépes infrastruktúrát csak rendeltetésszerűen használhatják. Így különösen tilos más felhasználók tevékenységének zavarása, adatok illetéktelen és jogosulatlan megszerzése, használata, a szoftverek és a hardver elemek megrongálása, működőképességük veszélyeztetése.

A felhasználó köteles a megkötött informatikai szolgáltatási szerződésben meghatározott kapcsolattartóval együttműködni.

A jelen szabályzatban foglaltak, illetve az elvárható gondosság be nem tartásából, a nem rendeltetésszerű használatból adódó károkért a felhasználó anyagi felelősséget is visel. Ilyen esetekben a szolgáltató a felhasználót kiegészítő szankcióként a számítógépes infrastruktúra használatában korlátozhatja, illetve teljesen kizárhatja.

A Társaság számítógépes infrastruktúráját használó személyeknek legalább felhasználói szintű számítógépes ismeretekkel kell rendelkezniük.

## 7. ADATVÉDELMI SZABÁLYOK

A felhasználóknak tilos bármilyen adathordozóra adatokat lementeniük. Külső adathordozót (Pen drive, CD/DVD stb.), csak az Igazgatóság elnökének engedélyével csatlakoztathatnak a számítástechnikai eszközökhöz.

A felhasználó munkaállomásának elhagyása esetén a számítógépet zárolni kell.

Nem engedélyezett a személyes, munkához közvetlenül nem kapcsolódó állományok tárolása.

## 8. JELSZÓKEZELÉSEL KAPCSOLATOS SZABÁLYOK

- a jelszó minimum 8 karakter hosszú, kicsi, nagy betűket és számokat tartalmaz,
- a jelszavakat 3 havonta le kell cserélni,
- a jelszó semmilyen jól látható, vagy könnyen hozzáférhető helyre nem írható le,
- a jelszó más felhasználók, üzletfelek számára nem adható ki.

## 9. FELHASZNÁLÓK JOGAI ÉS KÖTELESSÉGEI

*A felhasználónak joga van:*

- tájékoztatást kapni a helyi felhasználói szabályokról,
- panaszt tenni a *szolgáltató* intézkedései ellen,
- a számára megítélt erőforrások biztosítását a *szolgáltatótól* kérni,
- a géphez hozzárendelt szolgáltatásokat a felhasználói kategóriába sorolástól függően igénybe venni.

*A felhasználó kötelessége:*

- a felhasználói szabályzatok betartása,
- a *szolgáltató* utasításainak végrehajtása,
- a gép felhasználásával kapcsolatos fontos események, hibák rögzítése, jelentése, különös tekintettel a vírus fertőzések gyanújára,
- más felhasználók figyelmeztetése a szabályzatok betartására, a nem rendeltetésszerű, ill. szabályzatokkal ellentétes használat megakadályozása és jelentése,
- az esetlegesen felfedezett biztonsági lyukak, problémák jelentése a *szolgáltatónak*.

*A felhasználónak kifejezetten tilos:*

- a gépek megbontása, a hardver konfigurációk megváltoztatása,
- az esetlegesen előforduló biztonsági lyukak, hiányosságok kihasználása,
- más felhasználók munkájának zavarása, anyagainak illetéktelen megtekintése, másolása,

- a hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása,
- meghibásodás esetén önhatalmúan a hiba elhárításának megkezdése (Először a szolgáltatót kell értesíteni, a hibajelenség minél pontosabb leírásával. A szolgáltató a szolgáltatási szerződésben szereplő határidővel a hibák kijavítását megkezdi.)
- tilos annak kísérlete, amely a felhasználó a számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzésére irányul. (Az ilyen illetéktelen kísérlet, vagy sikeres megszerzés a betöréssel, ill. a lopással azonos megítélés alá tartozik.)

## 10. ÜZEMELTETÉSRE VONATKOZÓ SZABÁLYOK

### *Általános üzemeltetési feladatok*

A társaság számítógépes infrastruktúrájának általános üzemeltetési feladatai szolgáltatási szerződés alapján kerülnek elvégzésre.

### *A szolgáltató feladat-, és határhörrei*

A számítógépes infrastruktúrára vonatkozó Informatikai Szabályzat megtartásáért a társaság titkárságának vezetője egy személyben felelős, a titkárságvezető felel a felhasználók és a szolgáltatási szerződés alapján a szolgáltatást végző közötti kommunikáció megfelelő biztosításáért, az üzemeltetés – szolgáltatóval együttműködésben történő – biztosításáért.

A hardver meghibásodásakor a javításról, cseréről a szolgáltató javaslata alapján a titkárságvezető közreműködésével az Igazgatóság elnöke dönt.

A szolgáltató, mint rendszermenedzser feladat- és hatáshörrei:

- a hálózati struktúra kialakítása, az új elemek becsatlakozásának szabályozása, engedélyezése, ellenörzése,
- a hardver–szoftver és hálózati hibák felderítése, az elhárításhoz szükséges intézkedések megtétele,
- a felhasználók szükség szerinti szakmai irányítása,
- a hálózati struktúra nyilvántartása, a becsatlakozó elemek regisztrálása, nyilvántartási adatok bekérése, begyűjtése,
- erőforrás hozzáférési engedélyek kiadása,
- hálózati információk terjesztése, a felhasználók tájékoztatása,
- a külső csatlakozások biztosítása,
- a mail szerver installálása, adminisztrálása, karbantartása.

## **11. AZ INFORMATIKAI RENDSZER ELEMEI**

A társaság hálózati operációs rendszere jelenleg: Windows 2011 SBS. A fájl szerver mind szervezeti (csoportok), mind felhasználói szinten is elérhető.

Az elsődleges háttértár biztonsági okokból tükrözött. Rendszeres biztonsági adatmentést minden hó 1. és 14. munkanapján a rendszergazdának el kell végeznie.

## **12. A HÁLÓZAT ÜZEMELTETÉSE**

A hálózat üzemeltetését – szolgáltatási szerződés alapján – a szolgáltató végzi. A hálózatra való csatlakozás műszaki feltételei a szolgáltató ajánlása alapján kerülnek kialakításra, majd bármilyen módosítások a szolgáltató ajánlásai alapján az Igazgatóság elnökének döntését igénylik.

## **13. BIZTONSÁGI SZABÁLYOK**

A rendszerekhez való hozzáférés az alábbiak számára biztosított:

- ügyvezetők

A fenti munka-, ill. szerepkörök tekintetében hierarchia nincs, a rendszerekhez való hozzáférés minden munkakörben megegyezik.

## **14. INFORMATIKAI BIZTONSÁGI KOCKÁZATELEMZÉS**

Az informatikai kockázatelemzésének elvégzését a társaság egyik Ügyvezető Igazgatója rendelheti és fogadja el.

Jelen szabályzat rögzíti, hogy a társaság mai kockázatvállalásai mellett, ügyszámot, ügyfélszámot is tekintve a vállalt kockázattal arányos módon működik, informatikai biztonsága megfelelő.

## **15. MENTÉSI REND**

A folyamatos működés fenntartására, az üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében az adatok, információk külső merevlemezre mentésére havonta egyszer kerül sor.

A társaság által használt MINI CRM rendszer esetében az adatok, információk mentése naponta történik, a társaság székhelyétől elkülönítetten.

A társaság levelezését, kommunikációját szolgáló rendszerrel, valamint az MINI CRM rendszerrel kapcsolatos üzletfolytonosságot külső szolgáltató biztosítja, a mentéseket külső szolgáltató végzi.

A társaság informatikai rendszerét a társaság méretére, ügyfeleinek és ügyleteinek viszonylag alacsony számára tekintettel alakította ki és az alkalmazott rendszer, valamint a használt MINI CRM alkalmazás minden tekintetben megfelel a társaság elvárásainak. Az informatikai rendszerének fejlesztésére, módosítására az „üzemméret” változása, ügyletek és ügyfelek számának növekedése esetén kerülhet sor.

## **16. BIZTONSÁGI OSZTÁLYBA SOROLÁSI REND**

A társaság a biztonsági osztályba sorolásnál az alábbi szempontokat veszi figyelembe:

- személyes adatok védelme
- ügyfeleink személyes adatai
- kötelező adatvédelmi előírások
- saját dolgozók személyes adatai

A fentiek alapján két kategóriát állapít meg:

1. védett (adósok személyes adatai, üzleti és banktitkot tartalmazó információk, kötelezően alkalmazandó adatvédelmi előírások)
2. szigorúan védett (saját dolgozók személyes adatai)

A társaság a szolgáltatóval kötött szerződés, illetve az alkalmazott MINI CRM rendszer biztosítja az informatikai rendszerben tárolt adatok, információk szoftver és hardver oldalról történő védelmét. Szoftver oldalról biztosított a társaság adatvédelmi szabályzatában, valamint jelen szabályzatban foglalt feltételek teljesülése. Hardver oldalról a szolgáltatóval kötött szerződés feltételei alapján történik a védelem, az eszköztartalékolás, javítás, csere, a hibajavítás megkezdése, elhárítás időigénye rögzített.

## **17. AZ ADATOK HOZZÁFÉRÉSI RENDJE**

A hozzáférési rend – vagy logikai hozzáférési rend - rögzíti mindazokat a rendszerváltozókat és beállítási értékeket, amelyek meghatározzák, hogy az adatokhoz csak az arra jogosultak férjenek hozzá. A hozzáférési rendet a szolgáltató a társaság megbízása alapján alakította ki, az rendelkezésre áll.



## **18. ADATGAZDA**

A társaság üzleti adatainak gazdája alapértelmezetten a társaság operatív vezetője, társaságunknál az egyik Ügyvezető Igazgató (Papi András).

## **19. AZ ALKALMAZOTT SZOFTVER ESZKÖZÖK JOGTISZTASÁGÁT BIZONYÍTÓ SZERZŐDÉSEK**

A társaság csak jogtiszt szoftvereket használ. A vonatkozó szerződések rendelkezésre állnak.

## **20. AZ EGYES MUNKAKÖRÖK BETÖLTÉSÉHEZ SZÜKSÉGES INFORMATIKAI ISMERETEK**

A társaság által használt rendszerekhez hozzáférő alkalmazottainak az alábbi informatikai ismeretekkel kell rendelkezni:

- Windows operációs rendszer felhasználói szintű ismerete,
- belső hálózati erőforrások kezelése,
- MINI CRM rendszer felhasználói szintű ismerete,
- Word, Excel professzionális szintű ismerete,
- Power Point ismerete,
- Adobe Reader ismerete,
- internethasználat,
- a társaság által használt/előfizetett információs rendszerek ismerete.

## **21. AZ INFORMATIKAI BIZTONSÁGI RENDSZER KÖTELEZŐEN ALKALMAZANDÓ KONTROLLJAI**

### **Szervezeti és működési rend, folyamatba épített ellenőrzés**

Tekintettel arra, hogy a társaság az informatikai szolgáltatást szolgáltatótól veszi igénybe, a MINI CRM rendszert, mint felhasználó alkalmazza, a számítástechnikai fejlesztés és üzemeltetés nem kapcsolódik össze, nincs összeférhetlenség, a felhasználói jogosultságok az alkalmazottakra vonatkozóan azonosak, egymás helyettesítése lehetséges és megoldott.

A társaság az üzleti működésének jellegére, nagyságrendjére figyelemmel alakította ki informatikai rendszerét, jelen szabályzatban meghatározva az informatikai rendszerrel, annak biztonságával kapcsolatos szabályait.

A társaság egyik Ügyvezető Igazgatója (Papi András) a felelős jelen szabályzatban a munkatársakra meghatározott szabályok megismertetéséért, elfogadtatásáért.

Az informatikai rendszer működésének ellenőrzését a Belső ellenőrzés végzi.

### **Informatikai ellenőrző rendszer**

A társaságnál informatikai ellenőrző rendszer külső szolgáltató igénybevételével működik. Az informatikai rendszer hibáinak észlelése és azok megszüntetése az üzletfolytonossági tervben meghatározottak szerint történik.

A társaság szolgáltatója

- hálózat felügyeleti rendszert működtet,
- behatolás detektáló/gátló rendszert működtet.

### **Archiválás**

A szolgáltató által végzett archiválás biztosítja, hogy az archivált anyagokat a társaság öt évig visszakereshetően, helyreállíthatóan megőrizni képes.

## **22. AZ INFORMATIKAI BIZTONSÁGI RENDSZER KOCKÁZATOKKAL ARÁNYOSAN KIALAKÍTANDÓ VÉDELMI KONTROLLJAI**

### **Az informatikai rendszer elemeinek azonosítása**

A társaság szolgáltatója rendelkezik a legfontosabb elemek, azaz az eszközök, folyamatok, személyek azonosításáról.

### **A biztonsági rendszer védelme**

A társaság szolgáltatója gondoskodik az informatikai biztonsági rendszernek a biztonsági kockázattal arányos módon történő védelméről.

### **Felhasználói fiókok adminisztrációja**

A társaság szolgáltatója a biztonsági kockázattal arányos módon gondoskodik a rendszer szabályozott felhasználói adminisztrációjáról. Szolgáltató köteles olyan védelmi rendszert kialakítani, amely biztosítja az illetéktelen behatolások rögzítését, automatikus figyelmeztetések megküldését.

### **Az adathordozók kezelése**

A társaság az adathordozók kezelése során betartja az adathordozókon tárolt adatok biztonsági besorolása szerinti kezelési előírásokat. Amennyiben egy adathordozó üzemből kivonása történik, a társaság szolgáltatója az adathordozót megsemmisíti.

## **Vírusvédelem**

A társaság biztonsági kockázatával arányos módon szolgáltatója által gondoskodik a rendszer biztonsági kockázattal arányos vírus- és más rosszindulatú program elleni védelméről. A szolgáltató olyan integrált végponti biztonsági programot működtet, mely alkalmas a vírusok és egyéb kártékony kódok kiszűrésére, olyan beállításokat alkalmaz, melyek biztosítják az automatikus frissítés és automatikus ellenőrzések heti egy alkalommal történő végzését.

Jelen szabályzat 2017. június. 21. napján lép hatályba.

Budapest, 2017. június 19.

(a hitelesített, aláírt Informatikai Szabályzat a Kft. székhelyén iktatásra került)