04908/2017

Szegedi Rendezvény- és Médiaközpont
Nonprofit Kft.
6721 Szeged Felső Tisza-part 2.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályba lépés napja: 2017. november 30.

Dátum	Készítette	Verzió	Leírás
2017. 11. 29.	RITEK Zrt.	1.0	Alap verzió.

TARTALOMJEGYZÉK

Szegedi Rendezvény- és Médiaközpont Nonprofit Kft. Informatikai Biztonsági Szabályzata

Általános rendelkezések

(1) Informatikai Biztonsági Szabályzat hatálya

a) Személyi hatály

Az IBSZ személyi hatálya kiterjed

- a Társaság valamennyi szervezeti egységére, fő- és részfoglalkozású dolgozójára, illetve a közcélú foglalkoztatásban résztvevőkre egyaránt,
- mindazon külső szervezetekre, személyekre, akik a Társaság informatikai eszközeihez hozzáférést kapnak.

A dolgozók személyes használatába adott eszközökről egyéb szabályzat rendelkezik.

b) Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed az elektronikus információs rendszerre, az általa kezelt adatvagyonra és a kapcsolódó alábbiak szerinti elektronikus információs rendszer elemekre:

- Elektronikus információs rendszerek által kezelt összes adatra,
- Elektronikus információs rendszerekre, annak életciklusában a részét képző mindazon informatikai eszközökre és IT infrastruktúra elemekre, amelyekkel az IT szolgáltatások biztosítása és az adatkezelés történik, beleértve az alábbiakat:
  - hardver eszközök,
  - alap és felhasználói szoftverek, licencek,
  - elektronikus információs rendszerek által használt hálózati és kommunikációs elemek
- Elektronikus információs rendszerekhez igénybe vett szolgáltatások és a külső elektronikus információs rendszerek kapcsolatát biztosító hardver és szoftver elemekre, IT megoldásokra,
- Elektronikus információs rendszerek működését biztosító eszközök fizikai környezetére,
- Elektronikus információs rendszerek fejlesztése, üzemeltetése, karbantartása, támogatása és használata során felhasznált adathordozókra, amelyekkel az elektronikus információs rendszerhez kapcsolódó adatok kezelése történik,
- Be/kimeneti dokumentumokra, valamint az elektronikus információs rendszerek üzemeltetési, biztonsági és egyéb dokumentációira.

c) Érvényesség és felülvizsgálat

Jelen IBSZ a jóváhagyás napján lép hatályba.

Az IBSZ jelen verziója a következő verzió kibocsátásáig vagy visszavonásig érvényes.

Védelmi intézkedések

(1) Vegyes intézkedések

a) Szervezeti szintű alapfeladatok

Az információbiztonsági rendszerhez kapcsolódó legfontosabb szerepkörök, feladatok, felelősségek a következők.

Cégvezető

Feladatai, felelősségei:

- gondoskodik a kockázatok felméréséről, valamennyi információs rendszerre és kezelt adatra kiterjesztéséről, a kockázatok megfelelő kezeléséről, a felmérés és kezelés napra készen tartásáról,
- gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:
    - kiadja a Társaság elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
    - gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Társaság munkatársai információbiztonsági ismereteinek szinten tartásáról,
    - rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Társaság elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
    - gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
    - biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
    - gondoskodik arról, hogy az Ibtv-ben foglaltak az elektronikus információs rendszer fejlesztésében, üzemeltetésében, karbantartásában, auditálásában, vagy az adatkezelési, adatfeldolgozási tevékenységben közreműködő külső partner megállapodásokban szerződéses kötelemként teljesüljenek,
    - felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
    - megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket;

- a szervezeti felépítés, vagy szervezeti szintű architektúra kialakításánál figyelembe veszi a szervezet működését befolyásoló kockázati tényezőket (pl. tevékenységek szétválasztásánál, felügyeleténél),

Gazdasági Vezető

Feladatai, felelősségei:

- pénzügyi erőforrások biztosítása,
- költségvetés tervezés, és a beruházások, beszerzések során tervezi a szükséges forrásokat,
- intézkedik a terveknek megfelelő kiadásokhoz szükséges erőforrások rendelkezésre állásának biztosítása iránt,
- gondoskodik a Társaság informatikai eszközei és alkalmazásai leltárának napra készen tartásáról az informatikai munkatárs által kitöltött és átadott bizonylatok, átadás-átvételi jegyzőkönyvek, selejtezési jegyzőkönyvek alapján,
- gondoskodik a beszerzett eszközök és alkalmazások állományba vételéről,

Informatikai munkatárs

Feladatai, felelősségei:

- ellátja az szervezet informatikai feladatait
- kapcsolatot tart az Társaság dolgozóival, folyamatosan gyűjti a felmerülő igényeket, feladatokat,
- a Társaság információs rendszereit érintő jogszabályváltozások, illetve információs rendszerekre vonatkozó igények felmerülése esetén javaslatot tesz fejlesztésekre, közreműködik a megfelelő partner kiválasztásában, a feladatok specifikálásában,
- koordinálja a Társaság információs rendszerivel kapcsolatos fejlesztési beruházásokat, ellenőrzi a teljesítéseket,
- kidolgozza/kidolgoztatja a Társaság informatikai szabályzatait, ezek szükséges aktualizálásait, koordinálja annak betartására irányuló tevékenységeket,
- irányítja a Társaság információs rendszereinek működtetését,
- ellenőrzi, hogy a felhasználók az informatikai eszközöket a szabályozásokkal összhangban használják-e,
- részt vesz a Társaság hardware és software beszerzéseinek előkészítésében,
- folyamatosan tájékoztatja felettesét a folyó ügyek állásáról, az ügyekkel kapcsolatos problémákról, alternatívákat készít a megoldás lehetőségeire.

Szervezeti egységek vezetői

Feladatai, felelősségei:

- jelen szabályzatban meghatározott felhasználói azonosítás-hitelesítési és fiókkezelési eljárás során kezdeményezi a szervezeti egységébe tartozó munkavállalók szervezeti egységhez kapcsolt jogainak beállítását, módosítását illetve megszüntetését.

b) Viselkedési szabályok az interneten

A Társaság meghatározta a felhasználói viselkedésmódra vonatkozó legfontosabb szabályokat:

- tilos a szervezettel kapcsolatos bizalmas/nem nyilvános információkat írásos engedély nélkül az interneten nyilvánosságra hozni,
- az információs eszközöket csak az előírások szerint, csak az engedélyezett módon, célra szabad használni,
- az adatok kezelésére, információk továbbadására vonatkozó, előírásokat, korlátokat be kell tartani,
- be kell tartani a bizalmassági és titoktartási előírásokat,
- internet hozzáférés csak Társasági célokból történhet,
- tilos nem Társasági célú videó fájlok nézése, webrádió hallgatása, fájlcsere,
- tilos az internetről a munkavégzéshez nem szükséges állományokat letölteni, tilos az interneten biztonsági kockázatokat jelentő oldalakat látogatni,
- tilos közösségi oldalakon a Társaságot rossz fényben feltüntető információkat közzétenni,
- tilos közösségi oldalon Társasági véleményként értelmezhető magánvéleményt közzé tenni,
- a felhasználónak tilos a Társasági informatikai eszközökön szoftvert telepíteni,
- tilos a védelmi szoftverek (tűzfal, vírusirtó, stb.) beállításainak módosítása, funkcióinak kikapcsolása
- tilos a Társasági eszközökre, vagy a Társasági hálózatra nem a Társaság tulajdonában lévő eszközt csatlakoztatni (pl. felhasználói pendrive, mp3 lejátszó, laptop, stb.)
- tilos az informatikai eszközöket (a mobil használatra szánt eszközök kivételével) engedély nélkül áthelyezni, mozgatni,
- tilos a Társaság eszközét engedély nélkül másnak átadni,
- tilos engedély nélkül a hálózatra új eszközt kapcsolni.

Kockázatokkal arányosan, szükség esetén az informatikai munkatárs korlátozhatja a webtartalmak elérését, a Cégvezetővel egyeztetve.

<u>Az elektronikus levelezés szabályai:</u>

- tilos a gyanús című, vagy küldőtől érkezett e-mailek mellékleteinek, vagy az e-mailben található linkek megnyitása
- a Társasági e-mail postafiók használatával kiküldött e-mail esetében minden esetben biztosítani kell a Társaság jó hírnevét,
- a Társasági e-mail postafiók magán levelezés céljára nem használható,
- Társasági dolgozók a munkavégzéshez csak a Társasági postafiókot *(@ihrk.hu végződéssel)* használhatják,
- tilos a Társasági munkavégzéshez ingyenes e-mail szolgáltatások használata (pl.: gmail.com, freemail.hu, citromail.hu, stb.),

c) Szoftverbeszerzésnél a fentiek mellett figyelembe kell venni:

- célszerűségi, gazdaságossági és informatikai szempontokat az érintett felhasználók bevonásával,
- a szoftvergyártó cég rendelkezik-e megfelelő referenciákkal;
- funkcionálisan a program kielégíti a feladat igényeit, nem tartalmaz-e aránytalanul sok felesleges egyéb funkciót,
- milyen létszámú és milyen felkészültségű kezelőszemélyzetre van szükség a használatához,
- biztosított-e a szoftver nyomkövetése, azaz a jogszabályi változásokat nyomon követik-e, az így született verziókat milyen feltételek mellett bocsátják a Társaság rendelkezésére,
- amennyiben a Társaságnak egyedi programmódosítási igényei lennének, azt a gyártó vállalja-e és milyen feltételekkel,
- a gyártó cég milyen segítséget tud nyújtani a program bevezetésében, az üzemeltetés során felmerülő hibák, üzemzavarok elhárításában,
- milyen hardvert igényel a program üzemeltetése,
- a program nyújtotta szolgáltatások arányban vannak-e a szoftver árával,
- a szoftver használatához a gyártó milyen minőségű dokumentációt mellékel.

Az új szoftverek beszerzése az informatikai munkatárs feladata.

d) Emberi tényezőket figyelembe vevő – személy – biztonság

Az információbiztonsági rendszer kulcsszereplője az ember, így kiemelt jelentőségű az emberekkel kapcsolatos kockázatok csökkentése.

A Társaság minden munkatársa rendelkezik munkaköri leírással, mely tartalmazza a feladatokat, felelősségeket, ahol releváns, a biztonsággal kapcsolatosakat is. A munkaköri leírások elkészítését a HR munkatárs koordinálja, bevonva az érintett szervezeti egység vezetőket, információbiztonsági szempontból kiemelt munkakörök esetén az információbiztonsági felelőst is. A munkaköri leírásokat szükség esetén (pl.: a szervezet, illetve a munkakör változásakor) felül kell vizsgálni.

Információbiztonsági szempontból kiemelt munkakörök:

- Cégvezető
- HR munkatárs
- Szervezeti egység vezetők
- Informatikai munkatárs

A Társaság szabályozta az új dolgozó beléptetési folyamatát, mely kiterjed a munkavégzéshez szükséges eszközök átadására, a munkavégzéshez szükséges hozzáférési jogosultságok kiosztására, illetve a titoktartási nyilatkozat aláírására. A belépési folyamatot „sétálópapír" dokumentálja.

Eljárás a jogviszony megszűnésekor

A Társaság szabályozta a kilépési folyamatot is, mely kiterjed valamennyi átadott eszköz visszavételére, a hozzáférési jogosultságok megszüntetésére, az információknak a tevékenységet átvevő kollégának átadására, a titoktartási kötelezettségek kilépés utáni megmaradására. A kilépési folyamatot „sétálópapír" dokumentálja.

Az informatikai munkatárs a kilépő dolgozó munkakörének átadás-átvételekor megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerekhez.
Amennyiben a dolgozó részére korábban kiadásra került egyéni hitelesítő eszköz (pl.: digitális aláírásra alkalmas token, stb.), vagy a Társaság tulajdonát képező egyéb eszköz, az informatikai munkatárs a kilépő dolgozó munkakörének átadás-átvételekor ezeket az eszközöket is dokumentáltan visszaveszi.

A szervezet tájékoztatja a kilépőt a jogviszonya megszűnése után is fennálló titoktartási kötelezettségéről.
Az informatikai munkatárs felelőssége, hogy a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz való hozzáférés lehetséges legyen, ameddig a szervezet számára ez szükséges.

Amennyiben fennáll a veszélye, hogy a munkaviszony megszüntetésével érintett dolgozó kárt okozhat (pl.: rendkívüli jogviszonyt megszüntető okok esetén) az elektronikus információs rendszerben (pl.: adatokat töröl, felülír, stb.) az informatikai munkatárs megelőző intézkedésként köteles azonnal hatállyal megvonni a rendszer hozzáféréseket az adott dolgozótól. Ilyen veszély esetén szintén azonnal hatállyal meg kell vonni a fizikai hozzáféréseket is (kulcsok, beléptetőkártya, stb.). Az átadott eszközök azonnali visszavételről is intézkedni kell dokumentált átadás-átvétel keretében.

A Társaság eljár az információbiztonsági előírások megsértőivel szemben. Ilyen esetben első ízben a közvetlen vezető személyes beszélgetés keretében, esetleg anyagi szankciók kíséretében hívja fel az érintett figyelmét a követelmények betartásának fontosságára. Ismétlődés, vagy súlyos kötelességszegés esetén a Társaság fegyelmi eljárást indít a Munka Törvénykönyvének előírásai szerint.

e) Képzések, képzési eljárásrend

Minden személy, aki hozzáférést kap információs rendszerhez, a hozzáférés megadása előtt képzést kap az információs rendszer rá vonatkozó követelményeiről, a betartandó szabályokról, a betartás fontosságáról, esetleges hiányosságok lehetséges következményeiről. A képzés része a beléptetési folyamatnak is. Új információs rendszer, funkció, eszköz bevezetésekor szükség esetén a bevezetési folyamat részeként kapnak szerepkörüknek megfelelő képzést az érintettek. A speciális funkciókat ellátók (pl. rendszer admin, vagy hozzáférés beállítási jogosultsággal rendelkezők) külön képzésben részesülnek.

A tudatosság fenntartása, fejlesztése érdekében az információbiztonsági felelős szükség szerint, de legalább évente frissítő képzéseket tart. Az oktatásokról minden

esetben jelenléti ívet kell készíteni. A jelenléti íveket az információbiztonsági felelős őrzi meg. A képzési eljárásrendet javaslat érkezése, illetve szükség szerint a szervezet felülvizsgálja.

f) Adathordozók védelme

A tevékenységekhez, a biztonságos működéshez szükséges adathordozókat az informatikai munkatárs szerzi be és adja át a felhasználóknak, elsősorban mentési célokra. Az adathordozók biztonságos kezelése, védelme (megőrzése, sérüléstől, illetéktelen hozzáféréstől megvédése) az adathordozó kezelőjének feladata.

Adathordozó tartalmát használatból kivonás, más személynek átadás előtt törölni kell legalább Gutmann vagy azzal egyenértékű algoritmus alkalmazásával. Adathordozó selejtezése fizikai tönkretétellel történik, illetve elektromos hulladékként gyűjtés után megsemmisítő szakcégnek vagy az Önkormányzat informatikai cégének (RITEK Zrt.) kerül átadásra.

Számítógépek selejtezése, magánszemélyeknek vagy szervezeteknek átadása előtt az informatikai munkatárs vagy eltávolítja a háttértárat, vagy gondoskodik a háttértár törléséről (lásd előző bekezdés), újra formázásáról.

g) Azonosítás és hitelesítés

Az adatokhoz, információkhoz való hozzáférést a számítógépes felhasználói rendszerben a bejelentkezési azonosító (ID) és belépési jelszó (PW) páros használata teszi lehetővé.

Az azonosítókat a munkatársaknak az informatikai munkatárs belépéskor a humán erőforrás szervezet jelzése alapján adja ki, illetve kilépéskor az azonosítót inaktiválja (zárolja). Külső felhasználó esetén az illetékes szervezeti egység vezető írásos kérelmére történik az azonosító képzése, kiadása. A kérelmező szervezeti egység vezető felelőssége az azonosító visszavonásának kérése, ha már nincs szükség a hozzáférésre. Az azonosítok szerepkörök és szervezetek szerinti csoportokhoz vannak hozzárendelve. A felhasználók azonosításához, hitelesítéséhez az azonosítón felül jelszó szükséges.

A rendszerbe első belépéskor, amennyiben a rendszer ezt támogatja a kapott induló jelszót meg kell változtatni. A jelszó elfelejtése esetén kérni kell az informatikai munkatárstól a jelszó érvénytelenítését, és induló, megváltoztatandó jelszóra visszaállítást. Jelszó kiszivárgása (vagy ennek gyanúja) esetén a jelszót a felhasználónak haladéktalanul meg kell változtatnia.

A felhasználóknak a belépési jelszavaik kialakítása és használata során az alábbi jelszóképzési alapvető szabályokat kell figyelembe venni:

- általános szabály, hogy a jelszavak legalább 8 karakterből álljanak, tartalmazzanak számot és betűt is. 3 havonta cserélni kell a jelszót, szükség esetén az Informatikai Osztály dolgozóinak segítségét kérve.,
- törekedni kell arra, hogy a jelszó minél hosszabb legyen, és minél kevésbé hasonlítson a jelszó egy valódi szóhoz.,

- a jelszavak lehetőleg kis- és nagybetűt és számot is (esetleg speciális karaktert) tartalmazzanak,
- a jelszó ne kötődjön tulajdonosához (saját, családtag és háziállatok neve, cím, telefonszám, rendszám, születési dátum stb.),
- mindezek ellenére a jelszó legyen megjegyezhető,
- munkaállomások esetén az ékezetes karakterek használata célszerű (a jelszótörő programok többsége külföldi eredetű és ezek legtöbbje nem kezeli a magyar ékezetes karaktereket),
- a felhasználóknak gondoskodniuk kell jelszavaik kiszivárgásának megakadályozásáról:
    - ügyeljenek arra, hogy mások a jelszó beírását ne lássák,
    - belépési azonosítóikat, jelszavaikat sem egymásnak, sem idegen személynek nem adhatják át,
    - jelszavaikat lehetőleg ne írják fel, vagy ha mégis leírják, tárolják azt biztonságos helyen, papír esetében zárt szekrényben, fájl esetén jelszóval és titkosítással védve,
    - telefonon semmilyen körülmények között se adják ki belépési azonosítójukat, jelszavaikat.

Az azonosítás, hitelesítési adatokat a rendszerben, illetve az azonosítási, hitelesítési folyamat során a rendszerek védetten, fedetten kezelik, tárolják.

h) Rendszer és információ sértetlenség

A Társaság által üzemeltetett információs rendszereket az informatikai munkatárs üzemelteti. Ha a rendszerben hibát észlel, akkor intézkedik az elhárításról, a hiba jellegétől függően elvégzi a javítást, vagy elvégezteti a rendszer fejlesztését, támogatását végző külső szervezettel. A javítás éles üzembe állítása előtt teszteli a frissítés megfelelőségét, azt, hogy nincsenek-e nemkívánatos hatásai. Ha a javításra biztonsági rés bezárása miatt van szükség, a lehető leghamarabbi üzembe állításról kell gondoskodni.

A Társaság vírusvédelmi szoftvert használ a rosszindulatú kódok, vírusok elleni hatékony védelem érdekében. A licence kódot az informatikai munkatárs tárolja és gondoskodik az érvényességéről. A kód a felhasználóknak nem adható ki. A vírusvédelem kiterjed a Társaság minden számítógépére. A vírusvédelmi rendszer működtetése, a vírusmentesítés az informatikai munkatárs feladata.

A vírusfertőzések elkerülése érdekében be kell tartani az alábbi szabályokat:

- szoftvert kizárólag az informatikai munkatárs dolgozói, illetve a Társasággal szerződött beszállító vagy szoftverfejlesztő cég szakemberei telepíthetnek. Semmilyen magánjellegű, előzetesen nem engedélyezett program nem futtatható a Társaság számítógépein,
- minden számítógépen megfelelő tűzfalnak és aktív vírusvédelemnek kell üzemelnie; ha a tűzfal kikapcsolt állapotban van, vagy ha a vírusvédelmi szoftver nem frissül a felhasználónak az informatikai munkatárs felé haladéktalanul jeleznie kell,

- vírusfertőzés észlelése esetén haladéktalanul abba kell hagyni a munkát, és szólni kell az informatikusnak, aki gondoskodik a vírus szakszerű eltávolításáról,
- az internetről kizárólag a napi munkához szükséges anyagok tölthetők le, a származási hely ellenőrzése mellett; kétség esetén az informatikai munkatárs segítségét kell kérni,
- az internetről futtatható állományt letölteni csak az informatikai munkatárssal egyeztetve lehet,
- az elektronikus levelekhez csatolt, nem hitelesített állományokat, az ismeretlen forrásból származó (Spam) leveleket haladéktalanul törölni kell,
- Naprakész vírusvédelmi szoftver és bekapcsolt tűzfal nélkül számítógépet üzemeltetni tilos.

Az informatikai munkatárs munkatársai – a kockázatokkal arányos mértékben – figyelemmel kísérik a rendszerek működését, a rendszerüzeneteket, napló bejegyzéseket. A tűzfal naplók alapján figyelemmel kísérik az internet használatot. A letöltések számának növekedése, filmek letöltése esetén felveszi a kapcsolatot az illetővel.

i) Rendszer és kommunikáció védelem

A Társaság kialakította hálózati struktúráját, hálózaton belüli és kívüli kommunikációs csatornáit. Az alkalmazások esetén a rendszer tervezése során kerülnek meghatározásra a szükséges elkülönítési, illetve interfész követelmények. Az informatikai munkatárs feladata a hálózat felügyelete, a működőképesség, a dokumentációnak megfelelő működtetés biztosítása, a külső üzemeltetőkkel való együttműködés. A belső hálózat védelmét szoftveres tűzfal biztosítja. A beállításokat az informatikai munkatárs egyezteti a tűzfalat szállító szervezet szakembereivel.

j) Biztonsági események kezelése

Az információbiztonsági eseményeket az informatikai munkatárs – együttműködve az cégvezetővel – kezeli, felügyeli.

Az informatikai munkatárs figyelemmel kíséri az információs rendszerek működését, a riasztásokat, fogadja a felhasználói bejelentéseket. A Társaság minden külső és belső munkatársának feladata, hogy jelezze az informatikai munkatársnak, ha információbiztonsági eseményt, vagy gyengeséget észlel. Az informatikai munkatárs dokumentálja az információbiztonsági eseményekről az információkat, mind az általa feltártakat, mind a kapott jelzéseket.

Az informatikai munkatárs elemzi az esemény jellegét, és hatáskörétől függően megkezdi az eseménykezelést. A szokásos eseményeket az informatikai munkatárs felkészültsége, illetve az egyes rendszerek dokumentációi alapján kezeli, vagy felveszik a kapcsolatot az információs rendszer, eszköz támogató partnerével (fejlesztő/karbantartó, gyártó), az elvégzett tevékenységeket, eseményeket dokumentálja. Ha az informatikai munkatárs nem rendelkezik kellő hatáskörrel a

döntéshez, elhárításhoz, javaslatot tesznek az illetékes döntéshozónak. Ha az esemény elemzéséhez, a szükséges intézkedések meghozatalához szükséges, szakértőt vonnak be a folyamatba. Az események kezelését, az intézkedések végrehajtását az informatikai munkatárs követi, felügyeli.

Jelen szabályzat 2017. december 1. napján lép hatályba, és visszavonásig érvényes.

Szeged, 2017. november 30.

Szegedi Rendezvény és Médiaközpont Nonprofit Kft. 2.
6721 SZEGED, Felső-Tisza part 2.
Adószám: 18457027-2-06
Raiffeisen Bank Rt.:
12067008-00104557-00100001

Jávorszky Iván
ügyvezető igazgató