Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

Mobil Adat Távközlési és Informatikai Szolgáltató Kft.

Székhely:1037 Budapest, Montevideo utca 3/b. III.em.1.

Adószám: 24212573-2-41

Cégjegyzék száma: 01-09-995858

Statisztikai száma: 24212573-6120-113-01

A Mobil-Adat Kft. MA-IBSZ Információbiztonsági Szabályzat_külsősök részére_v1.4

Érvényes: 2026.03.27-tól

Kelt: Budapest, 2026. március 27.

A Társaság cégjegyzésre jogosult tagja:

Elektronikusan aláírta:
Brasnyó Péter
2026-04-07 10:20:42 +0200

Brasnyó Péter

Ügyvezető

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

MA-IBSZ Külső felek részére elkészített kivonat (Információbiztonsági Szabályzat, külső kivonat)

Verzió	V_1.4
Kiadás Dátum	2021.03.04
Jóváhagyás Dátum	Lásd az aláíró lapon
Státusz	Végleges
Besorolás	- „Nyilvános” - **„Korlátozott”** - „Bizalmas”
Szerző	Black Cell Kft. Baranya Zsolt
Felülvizsgáló	Mobil Adat Kft. Muhoray Róbert
Jóváhagyó	Mobil Adat Kft. Brasnyó Péter
Felülvizsgálat	A dokumentumban meghatározott időpontban, de legalább minden évben egy alkalommal.

Verziókövetés

Verziószám	Frissítés dátuma	A módosítás oka	Módosítást végezte
V_1.0.	2021.03.04	Első kiadás	-
V_1.1.	2023.02.14	Korábbi módosítások átvezetése	Baranya Zsolt IBF
V_1.2.	2024.05.21.	Éves felülvizsgálat, frissítés	Baranya Zsolt IBF
V_1.3	2025.03.05.	Éves felülvizsgálat, frissítés	Baranya Zsolt IBF
V_1.4	2026.03.05.	Éves felülvizsgálat, frissítés	Baranya Zsolt IBF

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

Tartalom

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

A Mobil Adat Kft. Információbiztonsági Szabályzatának külső felek részére elkészített kivonata

A Mobil Adat Kft. (a továbbiakban: Szervezet) elkötelezett az általa fejlesztett, fenntartott, üzemeltetett és használt elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosításában, ezért a külső felek részére a következően megvalósítandó információbiztonsági szabályzat kivonat (a továbbiakban: IBSZ) kerül kiadásra. A jelen dokumentumban foglaltak megvalósításától egyedi esetekben, a felek által történt dokumentált egyezség alapján a kockázatok alacsony szinten tartása mellett van lehetőség. Azon előírások, amelyek adott külső félre nem relevánsak, nem kell megvalósítani.

1 Általános rendelkezések

1.1 Az IBSZ célja

Az IBSZ célja az elektronikus információs rendszerek, és az azokban tárolt, feldolgozott és használt adatok és információk megfelelő szintű adminisztratív, fizikai és logikai védelméhez szükséges előírásokat egységes keretbe foglalja, valamint a biztonságos működéshez és a megfelelő információbiztonsági szint fenntartásához általánosan betartandó alapvető szabályokat, alkalmazandó intézkedéseket és tevékenységeket meghatározza.

Az ezektől való eltérést, amely minden esetben kizárólag csak szigorítás és/vagy kiegészítés lehet.

Az IBSZ feladata védeni az elektronikusan és egyéb módon tárolt adatokat és információkat, az adatok tárolására-, feldolgozására-, továbbítására és archiválására szolgáló elektronikus információs rendszereket (a továbbiakban: EIR), rendszer- és architektúrális elemeket, adathordozókat, továbbá az említett elemek biztonságát és folyamatos működésük biztosítását.

Az IBSZ célja továbbá, hogy megismertesse a külső felekkel a Mobil Adat Kft. információbiztonsági elvárásait. Az elvárások jelen dokumentumban kerülnek kifejtésre részleteiben. A jelen dokumentum mellékletét képező információbiztonsági elvárás lista implementációjával is teljesíthető a Mobil Adat Kft. információbiztonság iránti igényének való megfelelés biztosítása. Minden esetben dokumentált módon el kell fogadnia a külső feleknek az IBSZ külsősök részére készített kivonatában szereplő elvárások alkalmazását, vagy az első mellékletben szereplő egzakt elvárás listát.

1.2 Az IBSZ hatálya és érvényessége

1.2.1 Az IBSZ kivonat személyi hatálya

Az IBSZ kivonat személyi hatálya kiterjed a Mobil Adat Kft-vel szerződéses kapcsolatban álló Szervezet minden munkavállalójára, a Szervezettel szerződéses, vagy egyéb módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodásokban foglalt személyekre és/vagy titoktartási megállapodásokban foglalt személyekre (a továbbiakban: külső felek), továbbá a Szervezet telephelyein tartózkodás idejére minden külső személyre, vendégre, akik a Mobil Adat Kft. adatihoz bármilyen formában hozzáférnek/hozzáférhetnek.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

1.2.2 Az IBSZ tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed a Mobil Adat Kft. releváns adatok kezelésére szolgáló minden hardver és szoftver elemre, továbbá papír alapú adat/információ hordozóra, valamint szóban elhangzó információra, mely a Mobil Adat Kft. üzleti tevékenységével kapcsolatba hozható.

1.2.3 Az IBSZ időbeli hatálya

Az IBSZ a jóváhagyást és kihirdetését követő napon lép hatályba, és visszavonásig érvényes.

1.3 Az információbiztonság szervezeti rendszere

A Szervezet információbiztonsági szervezetének vezetője az EIRVF – a Mobil Adat Kft. ügyvezetője. A Szervezet információbiztonságáért az IBF (Információbiztonsági felelős) a felelős.

A Szervezet valamennyi dolgozója, valamint a személyi hatályban felsorolt személyek és szervezetek egyaránt felelnek a számukra meghatározott mértékben az információbiztonság megfelelő szintű fenntartásáért.

Az információbiztonság szervezetrendszerében részt vevő személyek munkaköri leírásának, vagy szerződésének tartalmaznia kell a szerepköröket, melyek az IBSZ-ben meghatározásra kerülnek.

A szerződéses partnernek ki kell alakítania a saját információbiztonsági keretrendszerét a felelősségekkel és feladatokkal.

1.4 Fogalom meghatározások

Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

Információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát növeli vagy megszűnteti.

Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Elektronikus információs rendszer: adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

Biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az EIR-ben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az EIR által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Külső fél: a Mobil Adat Kft-vel szerződéses kapcsolatban álló Szervezet. Jelen dokumentumban többféle hivatkozással kerülhet megnevezésre a külső fél, például szerződéses partner stb. A szervezet munkavállalóira és partnereire vonatkozó szabályok.

1.5 Fizikai biztonság

1.5.1 Informatikai eszközök védelme

A Mobil Adat Kft. és a szerződéses kapcsolatban álló Szervezet az informatikai rendszer elemeit úgy helyezi el, hogy azok folyamatos üzemét a külső és környezeti hatások lehetőleg ne akadályozzák. A Mobil Adat Kft. székhelyén személy és vagyonvédelem szempontjait figyelembe véve az irodában kamerarendszer működik. A Mobil Adat Kft. adatainak és információinak védelme érdekében úgy kell kialakítani az adattárolók védelmét, hogy az a bizalmasság követelményeinek megfeleljen, vagyis csak az arra jogosult személyek férhessenek hozzá fizikailag a szerverekhez, egyéb architektúra elemekhez.

1.5.2 Számítógépes munkahelyek biztonsága

Az a személy, aki nem rendelkezik felhasználói jogosultsággal a Szerződéses partner vagy a Mobil Adat Kft. valamely EIR-jéhez, de feladatának elvégzése céljából belép olyan helyiségbe, ahol az informatikai hálózatra kapcsolt vagy hálózati kapcsolat nélküli munkaállomás van elhelyezve, csak és kizárólag a jogosult felhasználó kíséretében tartózkodhat ott. Ebben az esetben a kísérő felelős a jogosultsággal nem rendelkező személy mindennemű tevékenységéért.

Az elektromos áramellátásról az iroda bérbeadó és/vagy az üzemeltető gondoskodik. A szünetmentes tápegység tesztelése félévente egyszer meg kell, hogy valósuljon.

A számítógépes munkaállomás elhagyásakor a felhasználónak kötelessége operációs rendszer szintjén annak zárolása. Ennek elmulasztása esetén a zárolás 10 percen belül automatikusan meg kell, hogy történjen a jelszóval védett képernyő aktiválódásával.

A tiszta asztal – tiszta képernyő politika követelményeinek való megfelelés minden felhasználónak a saját felelőssége. Tilos olyan papír alapú dokumentumot a munkaidőn kívül a takarító személyzet által bejárható helyiségben hagyni, amely a Mobil Adat Kft. tevékenységéhez kapcsolódó bármilyen adatot, információt tartalmaz.

1.5.3 Dohányzás

Dohányozni kizárólag az épület arra kijelölt részén szabad, minden más helyen és esetben tilos a dohányzás.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

1.6 Eszközök biztonsága

1.6.1 Informatikai hálózatok biztonsága

A belső informatikai hálózat biztonsága érdekében a hálózathoz kizárólag a szerződéses partner vagy a Mobil Adat Kft. Információs Vagyonelem leltárában szereplő eszközöket lehet csatlakoztatni, tehát magán, vagy nem a szervezet által menedzselt eszközt tilos! Amennyiben szükséges külső eszköz hálózathoz történő csatlakoztatása, az minden esetben csak az EIRFV írásbeli engedélyével és a kockázatok előzetes értékelésével lehetséges, ha nem áll fenn magas kockázat.

Tilos a Szervezet informatikai hálózatához csatlakoztatott eszközt egyidejűleg más informatikai hálózathoz (például vezeték nélküli hálózathoz) csatlakoztatni. Adott eszköz egyszerre egy időben csak egy helyről csatlakozhat a Mobil Adat hálózathoz.

1.6.2 Internet használat

A szerződéses partner és a Mobil Adat Kft. a belső informatikai hálózatán a felhasználóknak kizárólag az egyes munkafeladatok ellátásához szükséges internethasználatot engedélyezi, a magán céllal látogatott weboldalak vagy az onnan letöltött adatok által okozott kárért a felhasználó a felelős. Az internetes viselkedési szabályok be nem tartásával okozott kárért minden esetben a felhasználó a felelős.

Tilos illegális és jogvédett tartalmak és fájlok letöltése, tárolása.

Tilos a nem munkavégzéshez kapcsolódó kommunikációban a Mobil Adat Kft-re vonatkozó bármilyen információ szerepeltetése.

A munkavégzéshez szükséges oldalak elérése, amennyiben nem engedélyezett valamely más szabály implementációja következtében, egyedi kérelem alapján beállításra kerülhet a felhasználó elektronikus levélben küldött kérelme alapján, ennek azonban dokumentáltnak kell lennie.

1.6.3 Elektronikus levelezés és fájlcsere szabályai

Az interneten folytatott levelezés nem feltétlenül biztonságos, ezért bizalmas dokumentumot vagy információt, személyes adatot nem engedélyezett a Szervezet hivatalos e-mail címeire küldeni (külsős e-mail címekről).

Az üres tárgysorral rendelkező e-maileknél vélelmezhető, hogy a levél veszélyes (vírust tartalmazhat), ebből adódóan tilos minden olyan e-mail kinyitása, mely üres tárgysorral érkezik, azt azonnal törölni kell (A törölt üzenetek közül is!), valamint tilos e-mail-t üres tárgysorral küldeni.

Tilos másolatként publikus e-mail címet (gmail, freemail, yahoo, stb.) megadni olyan levelek esetén, amelyek címzettje vagy a teljes cég vagy azon belül valamely email csoportnak vagy szervezeti egységnek íródnak. Nem minősül publikus e-mail címnek egy céges e-mail-formátum, ha valami@cégnév.hu vagy valami@cégnév.com formában szerepel.

A Mobil Adat Kft. a biztonságos fájlcsere megvalósításához a saját maga által üzemeltetett SharePoint oldalon hozhat létre a külső felek részére fájlcsere felületet, amely dedikáltan kerül létrehozásra. A jogosultságokat a Mobil Adat fájlok adatklasszifikációja határozza meg. Feltölteni a szerződő félnek van lehetősége, letölteni kizárólag a “Korlátozott” dokumentumokat van lehetősége. Ettől szigorúbb irányba eltérhet a Mobil Adat Kft., engedékenyebb irányba nem, csak az EIRFV dokumentált engedélyével. Más

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

szervezet által kínált SharePoint fájlcsere platform kizárólag másodlagos megoldásként jöhet szóba, amennyiben a külső fél biztosítani tudja a platform biztonságát tanúsítvánnyal.

1.6.4 Munkaállomások használatának biztonsága

A munkaállomásokhoz hardver eszközt, beleértve az adathordozókat is, csak az IT üzemeltetés csatlakoztathat. Az USB-n keresztül a felhasználók általi bármilyen eszköz csatlakoztatása tilos, ezt logikailag tiltani kell!

A Szervezet tulajdonát képező munkaállomásokon csak az engedélyezett-, a Szervezet Információs Vagyonelem Leltárában szereplő szoftverek telepíthetők és futtathatók a kijelölt adminisztrátorok által. Más szoftvert telepíteni, futtatni, használni csak az EIRFV külön engedélyével lehet. Az ettől eltérő cselekményért a külsős fél tartozik felelősséggel.

1.6.5 Távoli munkavégzés szabályozása, annak biztonsága

A Mobil Adat és a szerződéses partner lehetőséget biztosít az érintettek számára, hogy indokolt esetben a Szervezet belső hálózatát távolról is elérhessék. Ehhez a Szervezet VPN megoldást használ, amelyen keresztül elérhető a távoli asztali kapcsolat. A VPN szolgáltatás minden esetben két faktoros hitelesítéssel működik.

1.6.6 Hordozható/mobil eszközök használatának biztonsága

A hordozható/mobil eszközök alatt kell érteni mindazon infokommunikációs eszközt, amely működése nem helyhez kötött, különösen a laptop, tablet, mobiltelefon.

Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát. Tilos a hordozható/mobil eszközöket gépjárműben, idegen helyen felügyelet nélkül vagy egyéb látható helyen tartani! Repülőút vagy vonatút alatt a hordozható/mobil eszközöket kizárólag kézipoggyászként/kézipoggyászban lehet szállítani!

Az érvényes szabályok betartásáért, az eszközökön található adatok esetleges kiszivárgásáért, az eszköz elvesztéséért, eltűnéséért, megsérüléséért minden hordozható/mobil eszköz használója személyesen felelős, külsős fél esetén a szerződéses partner. Közös (több személy által használt eszköz) használatú eszköz esetén a rendeltetésszerű használatért az a személy felel, akit az EIRFV vagy a szerződéses partner erre a feladatra kijelölt személye kijelöl az eszköz felügyeletére.

Eltűnés, ellopás tényét az érintett személynek azonnal-, késedelem nélkül jelentenie kell az IT üzemeltetésnek és az IBF-nek, a Mobil Adat ügyvezetőjének bármely kommunikációs csatorna használata mellett.

A szerződéses partnernek szoftver Whitelist-et (fehér lista, az engedélyezett szoftverek listája) kell létrehozni, amely eszközön Mobil Adattal kapcsolatba hozható adat vagy információ érhető el. Csak az engedélyezett szoftverek futtathatók az adott eszközökön.

1.7 Adatok és adathordozók biztonsága

1.7.1 Mágneses, optikai, elektronikus adathordozók kezelésének szabályai

A következő eszközök tartoznak ebbe a csoportba:

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

- Mágneses adathordozók: merevlemez, szalagos adathordozó stb.
- Optikai adathordozók: CD, DVD, VCD stb.
- Elektronikus adathordozók: általában flash memória alapú, például: SSD, USB pendrive, memória kártya, smart kártya stb. (a továbbiakban együtt: elektronikus adathordozók)
- Hitelesítő eszközök

Jogvédelem alá tartozó adathordozók másolása csak az EIRFV előzetes engedélyével lehetséges.

A hitelesítő eszközök (jellemzően belépő kártya, token), érvényessége a fizikai belépési jogosultság fennállásáig tart, ezt követően a belépő kártya érvényességét le kell tiltani. A logikai belépéshez használt tokenek tekintetében - függetlenül attól, hogy szervezeti mobil eszközön vagy saját mobil eszközön van – szükséges annak eltávolítása és a jogosultság megszűntetése. A használati ideje a hitelesítésre szolgáló eszközöknek a jogviszony fennállásáig tart, de legfeljebb a gyártó által meghatározott ideig, ezt követően frissíteni vagy változtatni kell a gyártó ajánlása szerint.

1.8 Szoftverek biztonsága

1.8.1 Programok telepítése, használata

A munkavégzést segítő-, szakmailag indokolható szoftver telepítését kérheti az IT üzemeltetés munkatársaitól elektronikus levél (e-mail) formájában.

1.9 Hozzáférések kezelése

A hozzáférési jogosultságok tekintetében a Szervezet a „Least Privilege” elv alkalmazásával jár el, vagyis minden érintett csak a feladata elvégzéséhez szükséges mértékben kaphat jogosultságokat.

1.10 Jelszó menedzsment

Minden felhasználó az infokommunikációs és hordozható/mobil eszközöket (eltérő rendelkezés hiányában) csak saját nevével és jelszavával belépve használhat. Külső (nem a Szervezet munkatársa) személy csak a Mobil Adat Kft. Felhasználója általi személyes helyszíni vagy írásos előzetes beleegyezésével használhatja a Mobil Adat Kft. által üzemeltetett munkaállomást.

1.10.1 Jelszószabályok

A jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben. (A szerződéses partnereknek saját információs rendszereiben ki kell kényszeríteni a következőket.)

Előzőekre tekintettel:

- A felhasználói jelszót TILOS mások által is hozzáférhető vagy látható helyre leírni vagy más számára kiadni!

- A felhasználó felelős minden olyan káreseményért, melyet az ő felhasználói fiókjának felhasználásával követtek el a felhasználó hibájából (pl. a felhasználóra vonatkozó szabályozások be nem tartása), beleértve a nap végén vagy inaktív állapotban esetlegesen bekapcsolva vagy zárolatlanul – programokból, hálózatból nem kijelentkezve – hagyott gépeket. A felhasználói jelszavak sem a Szervezeten belülre, sem kívülre, még kérésre sem adhatók ki. Tilos a felhasználói azonosítók egymás közti

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

átadása, valamint idegen jelszóval történő bárminemű gép- program, illetve alkalmazás használat. Más azonosítóadatával történő hálózati bejelentkezés fegyelmi eljárást von maga után.

- Ha bármilyen jel arra mutat, hogy a jelszó kompromittálódhatott, azonnal meg kell változtatni, és a visszaélésről tájékoztatni kell az IT üzemeltetés munkatársait és az IBF-et, továbbá a Mobil Adat Kft. ügyvezetőjét.

- A Szervezetnek joga van szükség esetén (pl. incidens, biztonsági esemény, kompromittált felhasználói fiók vagy annak gyanúja) felülírni a felhasználó jelszavát a felhasználó értesítése mellett.

- Nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre.

- A jelszó minél komplexebb, annál kisebb a valószínűsége, hogy visszaélést követnek el vele. Az alábbi szempontokat kell betartani:

  - legyen egyedi;
  - könnyen megjegyezhető, és nehezen kitalálható legyen;
  - semmi olyan dolgon ne alapuljon, aminek alapján valaki kitalálhatja (ilyenek a nevek, telefonszámok, születési dátumok, stb.);
  - ne legyen a gépnévre vagy a felhasználó névre utaló;
  - ne legyen sorozat;

- a minimális jelszószabályok:
  - minimum 11 karakter hosszúnak kell lennie; privilegizált jogosultságok esetén 15 karakter hosszúnak;
  - a 3 alapvető karaktertípusból (angol kisbetű, angol nagybetű, szám) mindegyikből legalább egyet tartalmaznia kell;
  - legalább 90 naponként változtatni kell;
  - nem lehet a legutolsó 3 jelszó egyike sem;
  - nem tartalmazhatják a felhasználói fiók nevét vagy a felhasználó teljes nevének két egymás utáni karaktert meghaladó részletét;
  - 5 hibás jelszóbeadás után a rendszer legalább fél órára zárolja az account-ot;
  - a bonyolultsági feltételeknek a jelszavak létrehozásakor vagy módosításakor kell érvényesülniük;

- Az alkalmazás vagy rendszer/eszköz funkcionalitásainak és beállításainak biztosítani kell a jelszó szabályoknak megfelelő képességeket.

- A jelszó beíráskor a rendszer ne jelenítse meg a jelszót a képernyőn.

- A jelszógondozó rendszer tárolja elkülönítve a jelszót a rendszerben tárolt egyéb adatoktól.

- A jelszavak csak rejtjelezve tárolhatók az informatikai rendszerekben.

- A jelszavak a lokális hálózaton belül is csak rejtjelezetten továbbíthatók.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

1.11 Adminisztratív és dokumentum biztonság

1.11.1 Dokumentumok biztonsági osztályozása

A dokumentumok bizalmasságának besorolása egyaránt érvényes, mind a papír alapú, mind az elektronikus dokumentumokra, iratokra, feljegyzésekre.

A dokumentumok bizalmasságuk alapján a következő kategóriákba sorolandók be:

- Nyilvános: nyilvános iratok nem tartalmaznak semmilyen olyan információt, amelynek nyilvánosságra kerülése a Szervezet működésében fennakadásokat, presztízsveszteséget vagy egyéb hátrányt okozhat. Ezek az iratok rendszerint célzottan külsőfeleknek vagy a nyilvánosságnak készülnek.

- Korlátozott: vagyis általában belső használatra készülő dokumentumok, de partnerek által megismerhető, ha dedikáltan nekik készül. Kiadásuk külső fél részére lehetséges, de csak EIRFV írásbeli engedéllyel, és ellenőrzött tartalommal.

- A Szervezet bizalmas kategóriába sorolt dokumentumait külső felek részére tilos kiadni.

A dokumentumok biztonsági besorolását az iratokon, dokumentumokon látható módon fel kell tűntetni. Amennyiben nincs külön feltűntetve az iratok, dokumentumok biztonsági osztálya, abban az esetben „bizalmasként” szükséges kezelni. Nyilvánosként csak abban az esetben kezelhető egy dokumentum, ha azt a Szervezet biztonsági osztályozásra jogosult személye kifejezetten abba az osztályba sorolta.

1.11.2 Papíralapú dokumentumok biztonsága

A papír alapú dokumentumokat a biztonsági besorolásnak megfelelően kell kezelni, továbbá a nyilvánostól eltérő minősítésű dokumentum csak az EIRFV engedélyével hagyhatja el a szerződéses partner és a Mobil Adat Kft. irodahelyiségét változatlan formában.

1.11.3 Elektronikus dokumentumok biztonsága

Az elektronikus dokumentumokat a biztonsági besorolásnak megfelelően kell kezelni. Az elektronikus dokumentumok biztonsági besorolása alapvetően megfelel a papír alapú dokumentumok szempontjainak.

1.12 Személyekkel, partnerekkel kapcsolatos biztonság

1.12.1 Titoktartás

A Szervezettel szerződéses kapcsolatban álló partnereket és egyéb szervezeteket is titoktartási kötelezettség terhel, a velük kötött szerződésekben meghatározottak szerint. Külső felek esetén az együttműködési megállapodás titokvédelemre vonatkozó része képezi a felelősségre vonhatóság alapját.

1.12.2 Szerződések külső partnerekkel

Szerződés kötése esetén az érintett EIR-eket, hálózatokat, architektúra elemeket, és az azokat érintő kockázatokat, valamint az alkalmazott biztonsági eszközöket és eljárásokat, felelősségeket a felek között létrejött szerződésekben rögzíteni kell.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

A szerződéseknek tartalmaznia kell a részletszabályokat arra az esetre, ha a Szervezet Információs Vagyonelem Leltárában szereplő elemet a másik fél rendelkezésére bocsát, abban az esetben is, ha csak hozzáférések biztosítása történik valamely EIR-hez. A biztonságra vonatkozó előírások kötelező elemei a szerződéseknek. Minden esetben írásban kell történnie az átadás-átvételnek, vagy a hozzáférési jogosultság biztosításának.

A szerződéseknek tartalmaznia kell a biztonsági előírások megsértése esetére vonatkozó szabályokat és a szankciókat.

A szerződéseknek tartalmaznia kell a személyi változások esetén eszközölendő teendőket (például: munkatárs kilépése esetén az egyedi jelszavak, vagy hitelesítő eszközök visszavonása), az információbiztonságot érintő szerepköröket és felelősségeket. Amennyiben a felelősség megosztott, abban az esetben a részleteket minden esetben ki kell bontani, hogy az elszámoltathatóság elve ne sérüljön.

Szerződéses követelményként kell megkövetelni a partnerektől, hogy a Szervezet hálózatát vagy valamely EIR-jét távolról elérő személy vagy szervezet milyen védelmi intézkedést kell foganatosítson a távoli eléréshez igénybe vett munkaállomásokon, eszközökön (például: kártékony kódok elleni védelem).

A kommunikáció jellegétől függően, bizalmas információk kizárólag titkosított csatornán keresztül közlekedhetnek a felek között, melynek részleteit a Szervezet határozza meg.

Kötelező meghatározni a szerződésekben az incidensek és biztonsági események jelentésének részletszabályait. Ez jelenti a kapcsolattartó személyek és elérhetőségek, a bekövetkezett incidens vagy biztonsági esemény időpontját, helyét, hatását, várható hatását, a kockázatok mérséklésére megtett intézkedéseket, és kapcsolódó technikai adatokat, információkat. Azonnali jelentési kötelezettség csak a biztonsági esemény bekövetkeztére kell, hogy vonatkozzon, a részletes további információk az eseménykezelés után is tudomására hozható a másik félnek.

A szerződésekben minden esetben ki kell kötni az ellenőrzések lehetőségének meglétét, amely garanciát nyújt a védelmi intézkedések betartásának biztosítására.

1.13 Információs rendszerek működésének biztonsága

1.13.1 Támogatás, hiba bejelentés

Minden az IBSZ kivonat hatálya alá tartozó személy és szervezet bármilyen rendkívüli esemény, EIR működési hiba, rendellenesség észlelésekor haladéktalanul tájékoztatja az IT üzemeltetést, valamint az IBF-et és a Mobil Adat Kft. ügyvezetőjét. Személyes adatok vélhető érintettsége esetén a GDPR és az az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és a szervezet adatvédelmi szabályozási rendszerében foglaltak alapján szükséges eljárni.

A be nem jelentett hibákból származó károkért és következményekért minden esetben a bejelentést elmulasztó személy tartozik felelősséggel, a partner azonban a szerződés szerint felel a károkért.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

1.14 Rendszer és szolgáltatás beszerzés biztonsága

1.14.1 Külső elektronikus információs rendszerek szolgáltatásai

A külső EIR-rel együttműködő, a Szervezet által üzemeltetett EIR-eket üzemeltető személy feladata az alábbiak végrehajtása:

- Szerződéses kötelezettségként követelje meg, hogy a külső EIR-ek szolgáltatásai mindenben megfeleljenek a szolgáltatási szerződésben fentiek szerint meghatározott elektronikus információbiztonsági és a hozzá kapcsolódó szolgáltatásbiztonsági előírásoknak,
- Indokolt esetben kerüljön meghatározásra a vészhelyzet esetén azonnal bevonható helyettesítő szolgáltató az EIR szolgáltatási folytonosságának fenntartása érdekében,
- Határozza meg és a külső EIR-rel együttműködő a Szervezet által üzemeltetett EIR-ek felhasználói dokumentációjában foglalják írásba a felhasználók feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban,
- Külső és belső ellenőrzési eszközökkel ellenőrizzék, hogy a külső EIR szolgáltatója megvalósítja-e az elvárt védelmi intézkedéseket.

1.15 Monitoring és ellenőrzés

Az IBF jelen IBSZ kivonatban, és a vonatkozó szabályzatokban, eljárásrendekben foglalt kötelezettségek teljesítését ellenőrzi. Az ellenőrzés eredményeit minden esetben jegyzőkönyvbe foglalja, és az eredményeket felhasználja a Szervezet az IBIR fejlesztéséhez.

1.16 Kapcsolattartás információbiztonsági hatóságokkal, Eseménykezelő központokkal

Biztonsági esemény bekövetkezése esetén, amennyiben az EIRFV és az IBF úgy dönt, a Szervezet IBF-e bejelenti azt a Kiberbiztonsági Incidenskezelő Központnak. Ez főleg olyan esetben történhet meg, amennyiben a biztonsági esemény kezelése a Szervezet lehetőségein túlmutat, és a szerződéses külső partnerek segítsége sem elegendő a probléma megoldásához.

A biztonsági események bejelentése előtt az IBF egyeztet a bejelentés tartalmát illetően az EIRFV-el.

1.17. Mesterséges intelligencia és gépi tanulást használó megoldások használata

A Mobil Adat Kft. nem tiltja a mesterséges intelligencia és a gépi tanulás alapú szoftverek és megoldások (a továbbiakban: Generatív AI) használatát, azonban annak használatára vonatkozóan korlátozásokat vezet be:

- Kizárólag olyan generatív AI használható a munkavégzési tevékenység támogatására, amely ismert megoldás (pl. ChatGPT).
- Azon generatív AI használatához, amely regisztrációt igényel, tilos magán e-mail címmel regisztrálni, a Mobil Adat Kft. releváns adatainak védelme érdekében. Kizárólag a szervezeti e-mail címmel történő regisztráció engedélyezett, mivel a magán e-mail címmel történő regisztráció felett nincs kontrol.
- A generatív AI használatot be kell jelenteni a Mobil Adat Kft. ügyvezetője részére annak megnevezésével e-mailes formában, hogy az ÁSZF-ek kockázatértékelés szempontjából áttekintésre kerülhessenek az IBF által, szükség esetén a kockázatok csökkentése megtörténhessen.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

- Tilos Mobil Adat Kft. releváns adatainak, főleg ügyfélkörbe tartozó személyek személyes adatainak feltöltése, beírása a generatív AI használata során, mivel nem biztosítható az adatok kezelésének GDPR megfelelősége (Európai Unión és/vagy Európai Gazdasági Térségen kívüli szervereken történő adattárolás), valamint további felhasználási lehetőségei.

A fenti szabályok megsértése esetén a külső szervezetek felelősségre vonhatók a fegyelmi eljárásokra vonatkozó szabályoknak megfelelően, szervezet esetén a szerződésben foglalt szerződésszegési klauzulában foglaltak szerint.

Brasnyó Péter

Mobil Adat Kft. ügyvezető

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

1. melléklet

A Mobil Adat általános információbiztonsági elvárásai szerződő partnerével szemben

A Mobil Adat Kft. kötelezettsége az ISO/IEC 27001:2022 Információbiztonsági irányítási rendszer szabvány megfelelőségének biztosítása. Ennek megfelelően az alábbiakban felsorolt információbiztonsági elvárásokat kell teljesítenie a szerződő félnek (a továbbiakban: Szervezet).

A Mobil Adat Kft. elektronikus információs rendszereivel vagy bármely a Mobil Adat Kft. által kezelt adattal kapcsolatba kerülő személy tekintetében biztosítani köteles a Szervezet, hogy az információbiztonsági szabályok betartásra kerüljenek az érintettek által. Az érintettek cselekedeteinek nyomon-követhetőnek, visszakereshetőnek kell lennie. Az érintettek bármely okból a szervezettől történő távozása, vagy Szervezeten belül történő áthelyezése esetén biztosítani kell, hogy a Mobil Adat Kft-ről rendelkezésére álló adatokat és információkat nem adja tovább semmilyen körülmények között, kivéve, ha erre jogszabály alapján hatóság, bíróság vagy egyéb jogosult szerv nem kötelezi. Titoktartási kötelezettség teljesítésére irányuló dokumentum álljon rendelkezésre, melyben a felelősségek és a következmények is rögzítésre kerülnek.

A Mobil Adat Kft. elektronikus információs rendszeréhez (fizikai vagy logikai) jogosultsággal rendelkező személyek Szervezettől történő távozásáról a Mobil Adat Kft-t írásban értesíteni köteles a Szervezet. A tájékoztatásban ki kell térni a távozó személy nevére, és a távozás időpontjára.

A Szervezet, a Mobil Adat Kft-vel bármilyen kapcsolatban álló személyek, a Szervezettől történő távozása, vagy Szervezeten belül történő áthelyezése során köteles biztosítani, hogy a saját elektronikus információs rendszereiben elérhető Mobil Adat Kft-vel kapcsolatba hozható adatokhoz és információkhoz történő (fizikai és logikai) hozzáférést dokumentált módon megszűnteti.

A Szervezet biztosítja, hogy a Mobil Adat Kft. ügyvezetője előzetesen megküldött kérésére betekintést biztosít az információbiztonsággal kapcsolatos, jelen elvárások teljesítésének ellenőrzése céljából, a Mobil Adat ügyvezető igazgatója által kijelölt személy részére.

A Szervezet haladéktalanul értesíti a Mobil Adat Kft. szerződésben rögzített kapcsolattartóját (vagy helyettesítőjét) és ügyvezetőjét, amennyiben olyan incidens, vagy biztonsági esemény történik, amely érinti a Mobil Adat Kft-vel kapcsolatos bármely adatot vagy információt. Abban az esetben is fennáll a tájékoztatási kötelezettség, ha a szervezet sikeresen kezelte az eseményt, és nem került harmadik félhez olyan adat vagy információ, amely a Mobil Adat Kft-vel kapcsolatba hozható, továbbá, ha az adatok és információk rendelkezésre állása nem sérült.

A jelen szerződés tárgyát képező kötelezettség teljesítésében résztvevő személyekkel köteles a szervezet megismertetni jelen információbiztonsági elvárásokat, továbbá a Mobil Adat Kft. IBSZ kivonatban foglaltakat. Az elvárások megismertetését igazolható módon biztosítani kell a Szervezetnek a Mobil Adat felé ilyen irányú kérés esetén.

A Szervezet biztosítja, hogy belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

A Szervezet biztosítja, hogy kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más releváns jogszabályoknak.

A Szervezet biztosítja a másolatok, megosztások ellenőrzésének és a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatának nyomon követését.

A szervezet ellenőrzi és dokumentálja a Mobil Adat Kft-vel kapcsolatos állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

A Szervezet biztosítja a Mobil Adat Kft-vel kapcsolatba hozható adatok és információk sértetlenségének és bizalmasságának biztosítását adminisztratív, fizikai és logikai védelmi intézkedések implementálásával. A Mobil Adat Kft. ügyvezetője ezen kötelezettség teljesítésével és annak részleteivel kapcsolatban tájékoztatást kérhet a Szervezettől, feltételezhető nem megfelelőség esetén ellenőrizheti a Mobil Adat Kft. az elvárásoknak történő megfelelést.

A Szervezet azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit, amelyben jelen szerződésben meghatározott, a Mobil Adat Kft-vel kapcsolatba hozható adat vagy információ érintett.

A Szervezet a Mobil Adat Kft. adatai és információi védelme érdekében az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat. A Szervezet frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg. A Szervezet konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják. A kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és riassza a rendszeradminisztrátort és a Szervezet által meghatározott további személy(eke)t.

A Szervezetnek felügyelni kell az elektronikus információs rendszereit, amelyben a Mobil Adat Kft-vel kapcsolatba hozható adat vagy információ található, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat, továbbá azonosítania kell tudni a Szervezetnek az érintett elektronikus információs rendszer jogosulatlan használatát. Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

Abban az esetben, ha a Szervezeten belül bekövetkezett incidens vagy biztonsági esemény a Mobil Adat Kft. adatait vagy információit-, vagy a Mobil Adat Kft. által használt, de a Szervezet által üzemeltetett rendszert érinti, a Szervezet köteles bejelenteni az eseményt a Kiberbiztonsági Incidenskezelő Központnak, a Mobil Adat Kft. ügyvezetőjének megküldött értesítésével egyidejűleg.

Montevideo u. 3/B, Budapest, H-1037, Hungary
Tel: +36 1 88 99 100 Fax: +36 1 88 99 101

Ha a Szervezet az információbiztonsági kockázatainak elemzésekor olyan kockázatot tár fel, amely a Mobil Adat Kft-vel kapcsolatba hozható adatokat és információkat érinti, és a saját kockázatelemzési módszertanában meghatározott kockázati szint a maradványkockázatot illetően legalább közepes, vagy annál magasabb kockázat, köteles értesíteni a Mobil Adat Kft. ügyvezetőjét

A Szervezetnek meg kell határoznia az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is. A szerződő félnek meg kell felelnie a következő személybiztonsági követelményeknek: szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartás, összeférhetetlenség. Dokumentálni kell a személybiztonsági követelményeket és az azoknak való megfelelést, melyet a Szervezetnek rendszeresen ellenőriznie kell.