FOSTER Biztosítási Alkusz Kft

INFORMATIKAI ÜZEMELTETÉSI ÉS INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2019. január 31. napjától

Jóváhagyta:

Fazekas István
ügyvezető igazgató

FOSTER Biztosítási Alkusz Kft.
5600 Békéscsaba Munkácsy u. 2.II.3.
Adószáma: 11043900-2-04
Cégjegyzékszáma: 01-09-291888
Képviseletre jogosult személy: Fazekas István és Gonda József ügyvezető igazgatók

Jelen Szabályzatot (a továbbiakban: **Szabályza**t) a FOSTER biztosítási Alkusz Kft. (a továbbiakban: **Foster Kft**.) a belső információvédelmi folyamatainak szabályozása céljából alkotja. E **Szabályzat** rendelkezéseit a **Foster Kft. Adatvédelmi Szabályzatával**, és annak mellékleteivel, valamint többi szabályzatának, eljárásrendjének előírásaival összhangban kell értelmezni.

A **Szabályzatban** nem szabályozott kérdésekben a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.), AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) és a vonatkozó jogszabályi rendelkezések szerint kell eljárni. Amennyiben a **Szabályzat** rendelkezése – jogszabályváltozás okán – jogszabályi rendelkezésbe ütközne, minden esetben a hatályos jogszabályi rendelkezések az irányadóak, és haladéktalanul kezdeményezni kell a **Szabályzat** módosítását.

A **Szabályzat** felülvizsgálata és karbantartása az arra kinevezett ügyvezető igazgató hatáskörébe tartozik, és a jogszabályi változások függvényében, a változás hatályba lépését követő 90 napon belül történik. A szabályzatot legalább 3 évente, illetve szabályozott folyamatok lényeges változása esetén felül kell vizsgálni.

Tartalom

I. ÁLTALÁNOS RENDELKEZÉSEK

I.1. A Szabályzat célja és alapelvei

I.1.1. Jelen **Szabályzat** megalkotásának célja, hogy meghatározza a **Foster Kft.-**nél alkalmazandó intézkedéseket.

I.1.2. Az informatikai biztonság, az információvédelem elsődleges célja az információ bizalmasságának, sértetlenségének és rendelkezésre állásásnak megőrzése.

I.1.3. **Az információbiztonság alapelvei**:

I.1.3.1. ***Bizalmasság elve****:* minden esetben biztosítani kell, hogy az információhoz csak az arra jogosultak, csak az előírt módon férhessenek hozzá.

I.1.3.2. ***Sértetlenség elve***: minden esetben biztosítani kell, hogy az információt csak az arra jogosultak, csak szabályozott módon változtathassák meg. A sértetlenség biztosítása garanciát nyújt az információ teljességére és pontosságára.

I.1.3.3. ***Rendelkezésre állás elve***: minden esetben biztosítani kell azon állapot fenntartását, amely arra irányul, hogy az informatikai rendszer szolgáltatásai állandó jelleggel, illetve egy előzetesen meghatározott időben rendelkezésre álljanak, és a rendszer működőképessége átmenetileg se legyen akadályozva.

I.1.3.4. ***Hitelesség elve*:** az információ azon tulajdonsága, amely eredeti jellegét biztosítja.

I.1.3.5. ***Letagadhatatlanság elve***: garantálni kell az információ eredetét, a kézbesítés megtörténtét.

I.1.3.6. ***Funkcionalitás elve*:** minden esetben biztosítani kell a rendszer funkcionalitásának stabil, megbízható szolgáltatását.

I.2. A Szabályzat hatálya

Jelen **Szabályzat** személyi hatálya alá tartoznak az **Foster Kft**.-vel mint **Adatkezelőre** és annak munkavállalóira, illetve mind azokra, akiknek a munkavégzésük során kapcsolatba kerülnek az **Adatkezelő** által kezelt személyes adatokkal, valamint az **Adatkezelő** részére **Adatfeldolgozó** tevékenységet végző szerződéses partnerekre, függetlenül az adatkezelés/adatfeldolgozás céljától és módjától.

A **Szabályzat** tárgyi hatálya kiterjed a **Foster Kft**. valamennyi szervezeti egységénél, alvállalkozójánál folytatott valamennyi adatkezelésre és adatfeldolgozásra, valamennyi, a **Foster Kft.** és alvállalkozói tulajdonában vagy használatában, a rendelkezése alatt álló informatikai eszközre és programra, valamint minden olyan adatra, információra, amelyet a **Foster Kft**. működésével, tevékenységével összefüggésben kezel, feldolgoz, vagy azon bármilyen más műveletet hajt végre.

I.3. Értelmező rendelkezések

Adat: Az információ megjelenési formája, azaz tények, elképzelések nem értelmezett, de értelmezhető közlési formája. Jelen **Szabályzat** esetében az adat fogalmába beletartozik a **Foster Kft**. által kezelt minden információ és dokumentum, különösen ideértve az üzleti titoknak minősülő adatokat.

Adatállomány: Az egy nyilvántartásban kezelt adatok összessége.

Adatfeldolgozó: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

Adatgazda: a **Foster Kft.** azon szervezeti egységének a vezetője, ahol az adat keletkezik, az adatkezelésre vonatkozó döntési jogosultsággal rendelkezik, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére.

Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

Adatmegsemmisítés: Az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattovábbítás: Ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adattörlés: Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

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

Dokumentum: az ismereteket rögzítő információhordozó.

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

Felhasználó: A **Foster Kft**.-vel munkaviszonyban vagy munkavégzésére irányuló egyéb jogviszonyban (alvállalkozói) álló személy, aki a munkaviszonya alapján vagy

egyéb szerződéses keretek között a **Foster Kft.** infokommunikációs rendszeréhez hozzáfér.

Infokommunikációs (adatvédelmi) incidens: Az adat (nem csak személyes adat) jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

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.

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.

Megbízó/Ügyfél: Olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely **Alkuszi Megbízási Szerződéses** jogviszonyban áll a **Foster Kft**.-vel, és számára a **Foster Kft**. szolgáltatást nyújt.

Üzleti titok: a gazdasági tevékenységhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a jogosult jogos pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli.

II. A SZÁMÍTÁSTECHNIKAI INFRASTRUKTÚRA HASZNÁLATÁNAK SZABÁLYAI

II.1. A számítástechnikai infrastruktúra használatának általános szabályai

II.1.1. A **Foster Kft**. által a munkavállalók, és a **Foster Kft.-**vel munkavégzésre irányuló alvállalkozói szerződéses jogviszonyban álló személyek (a továbbiakban: **Felhasználók**) részére biztosított számítástechnikai infrastruktúra (a továbbiakban: számítástechnikai infrastruktúra) célja a munkavégzéshez szükséges feltételek biztosítása. A számítástechnikai infrastruktúra körébe tartozik jelen **Szabályza**t alkalmazásában a **Foster Kft** és az **Alvállalkozói** által használt hardver, illetve a saját és bérelt szoftverek, valamint az ezekhez kapcsolódó szolgáltatások is.

II.1.2. A számítástechnikai infrastruktúra és az informatikai rendszer üzemeltetéséért és biztonságáért felelős személyek (a rendszergazda vagy a szakmai vezető) a

Felhasználók előzetes tájékoztatása mellett, bármikor ellenőrizhetik a számítástechnikai infrastruktúrába tartozó eszközöket

II.1.3. Az informatikai eszközök tárolására szolgáló helyiségeket zárva kell tartani, ezekbe a helyiségekbe kizárólag az arra engedéllyel rendelkező személyek jelenlétében lehet belépni, és ott tartózkodni.

II.1.4. A rendszergazda feladata, hogy megakadályozza a **Foster Kft**. informatikai rendszerének erőforrásaihoz történő illetéktelen felhasználói hozzáférést.

II.2. Felhasználó kötelezettségei

II.2.1. A számítástechnikai infrastruktúrát valamennyi **Felhasználónak** rendeltetés-szerűen kell használnia.

II.2.2. A **Felhasználó** köteles együttműködni a rendszergazdával.

II.2.3. A **Felhasználónak** jeleznie kell a rendellenes működést és az egyéb általa veszélyesnek ítélt helyzeteket.

II.2.4. A **Felhasználó** felelős, hogy az adatfájlokat, dokumentumokat és adatbázisokat az adathordozó sérülésének veszélye miatt, a szükséges feladatok elvégzése után, kötelezően és haladéktalanul szerverre mentse.

II.2.5. A **Felhasználó** felel a titoktartási követelmények, titoktartási megállapodások, a vonatkozó jogszabályok betartásáért.

II.2.6. A **Felhasználónak** az informatikai szervezet által telepített vírusellenőrző programmal szükség esetén, de legalább három havonta teljes vírusellenőrzést kell végrehajtania a helyi eszközökön, továbbá felelős az infokommunikációs rendszerhez csatlakoztatott minden eszköz, valamint az Internetről letöltött anyagok vírusvédelméért.

II.2.7. A **Felhasználó** felel a jogszabálykövető és biztonságos Internet használatért.

II.2.8. A **Felhasználónak** tilos más felhasználók erőforrásait illetéktelenül használni.

II.2.9. A **Felhasználónak** a laptopok, „okos telefonok" és más hordozható mobil eszközök esetében különös gonddal kell eljárnia az eszköz és az azon található adatok és dokumentumok védelme érdekében, ezek nyilvános helyen semmilyen körülmények között nem hagyhatók őrizetlenül, használatuk átruházása tilos.

II.2.10. Tilos a nem engedélyezett szoftverek, filmek, zenék és más szerzői jogvédelem alá eső anyagok letöltése, másolása.

II.2.11. A hálózatba beléptetett munkaállomást tilos kilépés, illetve lezárás nélkül elhagyni.

II.2.12. Tilos a hálózati erőforrásokat védő technikai korlátozások feltörése, más **Felhasználók** jelszavaknak megszerzése.

II.2.13. Tilos a rendszer, és más **Felhasználók** adatait, fájljait — engedély nélkül - másolni, törölni vagy módosítani.

II.2.14. A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett **Felhasználó** a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat jogosulatlanharmadik személy hajtotta végre, amennyiben erre jelen **Szabályzat** előírásainak **Felhasználó** általi be nem tartása miatt kerülhetett sor.

II.2.15. Amennyiben a munkaállomást több személy is használhatja, a **Felhasználó** a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és az operációs rendszerből is kijelentkezett.

II.2.16. A **Felhasználó** dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott iratot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni — amennyiben szükséges, informatikus munkatárs segítségével — arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

II.2.17. A **Felhasználó** a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

II.2.18. Valamennyi **Felhasználónak** tilos:

- az általa használt eszközök biztonsági beállításait megváltoztatni,
- a számítógép rendszerszintű beállításait módosítani (ide nem értve az irodai programok felhasználói beállításait),
- a munkaállomására telepített aktív vírusvédelmet kikapcsolni,
- belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,
- a számítógép-hálózatot fizikailag megbontani, számítástechnikai eszközöket lecsatlakoztatni, illetve bármilyen számítástechnikai eszközt rácsatlakoztatni a hálózatra a rendszergazda jóváhagyása nélkül,
- a számítástechnikai eszközökből összeállított konfigurációkat megbontani, átalakítani,
- bármilyen szoftvert installálni, Internetről letölteni, külső adathordozóról merevlemezre másolni a rendszergazda engedélye, illetve közreműködése nélkül, a munkaállomásokon nem a **Foster Kft.** által rendszeresített, vagy engedélyezett szoftvereket (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálni és futtatni,
- online játékokat használni,
- bármilyen eszközt számítástechnikai eszközökbe szerelni és használni,
- az általa használt adathordozó (pl. CD, DVD, Pendrive stb.) eszköz számítógépben hagyni a munkaállomásáról való távozás esetén,
- ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni. Ilyen esetben az adathordozót teljes vírusellenőrzést kell

lefuttatni és csak a jóváhagyását követően lehet az adathordozót használni az eszközben,
- más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,
- láncleveleket továbbítani, levélszemetet, továbbá azok mellékleteit, vagy linkjeit megnyitni, rendszer biztonságáért felelős személy külön engedélye nélkül — feliratkozni, kivéve a munkavégzéshez szükséges: a **Foster Kft.** által megrendelt, működtetett, vagy előfizetett szolgáltatásokat, belső információs rendszereket, adatfeldolgozó szervek/szervezetek által biztosított szolgáltatásokat, és a szolgáltatások levelező listáit.

II.2.19. A **Felhasználó** felelős az általa használt számítástechnikai infrastruktúráért, azok biztonságáért és az azokon tárolt adatokért, dokumentumokért.

II.2.20. Abban az esetben, ha a **Felhasználó** valamely, a **Foster Kft**. tulajdonát képező információt, adatot olyan informatikai, infokommunikációs eszközön tárol, amely nem áll a **Foster Kft**. és vele szerződésben álló **Alvállalkozó** tulajdonában vagy használatában, külön területet kell kijelölni kizárólagosan a Foster Kft. adatainak tárolására. A rendszergazda a **Felhasználó** munkavégzésre irányuló és **Alvállalkozói** jogviszonyának megszűnése esetén távoli adattörléssel törli az kizárólagos területe lévő Foster információkat és adatokat, a **Felhasználó** személyiségi jogainak legmagasabb szintű védelmének biztosítása mellett.

III. AZ ADATKEZELÉST VÉGZŐK KÖRE ÉS JOGOSULTSÁGA

III.1. Adatfeldolgozó

Az adatfeldolgozó jogosultságának megfelelően jogosult az adatkezeléshez kapcsolódó műveletek elvégzésére. A kezelt adatokat a jogosultságtól eltérő módon senkinek nem adhatja át, azokról információt nem szolgáltathat.

III.2. Adatkezelő

Az adatkezelő jogosultságának megfelelően jogosult önállóan vagy másokkal együtt az adat kezelésének célját meghatározására, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntések meghozatalára, és végrehajtására, vagy az adatfeldolgozóval történő végrehajtására. A kezelt adatokat a jogosultságtól eltérő módon senkinek nem adhatja át, azokról információt nem szolgáltathat.

III.3. Ügyvezető igazgató

A **Foster Kft**. ügyvezető igazgatója a társasági szintű dokumentumok, adatok adatgazdája. Jogosult a **Foster Kft.** dokumentumainak, adatainak kezelésére. Jogosult az adattovábbításban, adattárolásban, adatfeldolgozásban szereplő

valamennyi adatba betekinteni, elemzés céljából azokat tovább feldolgozni, adatokat továbbítani.

III.4. Programozó

A programozó jogosult az adatok kezeléséhez szükséges adatállományok létrehozására, az elemzésekhez, lekérdezésekhez, adattovábbításhoz szükséges adatok kezelésére, programok, átmeneti állományok létrehozására.

III.5. Rendszergazda

A rendszergazda jogosult az adatokról biztonsági és archiválási másolatok létrehozására, tárolására.

IV. ADATOK ÉS DOKUMENTUMOK OSZTÁLYOZÁSA

Adott infokommunikációs rendszer által importált, feldolgozott, tárolt vagy exportált adatok és dokumentumok védelmi szintjének arányban kell állnia annak kockázatérzékenységi szintjével.

Az adatgazda felelős a hatáskörébe tartozó adatok osztályozásáért. Az adatok osztályozása segít meghatározni az adatvédelem alapvető biztonsági ellenőrzéseit, valamint felhasználható az infokommunikációs biztonságvédelem szintjének meghatározására.

Az alábbi négy besorolást kell alkalmazni az adatok kockázatérzékenységi szintjének osztályozásakor és kezelésekor:

- **Személyes adat:** Jelen Szabályzat I.3. pontjában meghatározott személyes adatnak minősülő adatokat „Személyes adat" kategóriába kell sorolni. Az információkezelés biztonsági szintje a legmagasabb szintű.
- **Üzleti titok:** Jelen Szabályzat I.3. pontjában meghatározott üzleti titok meghatározásnak megfelelő adatokat „Üzleti titok" kategóriába kell sorolni. Az információkezelés biztonsági szintje magas szintű.
- **Korlátozottan megismerhető:** az adatokat és dokumentumokat „Korlátozott terjesztésű!" kategóriába kell sorolni, ha a jogosulatlan közzététel, változtatás(ok) vagy megsemmisítés kellemetlenséget okoznak, ugyanakkor nem valószínű a pénzügyi veszteség vagy hitelesség sérülése. Alapértelmezés szerint korlátozott osztályba kell sorolni az összes adatot és dokumentumot, amelyet nem minősít a **Foster Kft.** bizalmasnak vagy nyilvánosnak. Az információkezelés biztonsági szintje ellenőrzött, alapértelmezett.
- **Nyilvános:** az adatokat és dokumentumokat „Nyilvános" kategóriába kell sorolni, ha a jogosulatlan közzététel, változtatás(ok) vagy megsemmisítés semmilyen vagy elfogadható szintű kockázatot jelent a **Foster Kft**. számára. Az információkezelés biztonsági szintje alacsony.

V. INFOKOMMUNIKÁCIÓS BIZTONSÁGI KOCKÁZAT ÉRTÉKELÉS

A **Szabályzat** kockázat alapú megközelítéssel biztosítja a **Foster Kft**. adataira és dokumentumaira vonatkozó megfelelő biztonsági elvárások meghatározását és az üzleti célokkal való összhangját.

Az infokommunikációs rendszer használatára, tulajdonlására, üzemeltetésére vonatkozó kockázatok üzleti kockázatok. Ezek különösen előfordulhatnak üzleti kihatással bíró biztonsággal kapcsolatos események esetében.

V.1. Infokommunikációs kockázatértékelés

A rendszergazda és az adatvédelmi tisztviselő az infokommunikációs kockázatokat szükség esetén, de legalább évente, minden év április 30. napjáig értékeli, kezeli és ellenőrizi, és erről írásban jelentést tesz a **Foster Kft.** ügyvezető igazgatójának szükség szerint, és minden év május 10. napjáig.

Formális kockázatelemzést kell végezni, amennyiben az adatgazda, az adatvédelmi tisztviselő vagy a rendszergazda indokoltnak tartja, valamint adatvédelmi incidens bekövetkezésekor.

A kockázatelemzés végrehajtása során:
A rendszergazda és az adatvédelmi tisztviselő költség-haszon alapú és az érintettekre gyakorolt hatást vizsgáló megközelítést alkalmaz, értékelve a kockázatok hatását és valószínűségét.
A rendszergazdának és az adatvédelmi tisztviselőnek figyelembe kell vennie a használt biztonsági ellenőrzések hatékonyságát.

A rendszergazda és az adatvédelmi tisztviselő meghatározza azon kritériumokat, amelyek segítik a megfelelő kockázatkezelési stratégia kiválasztását.

V.2. Kockázatkezelés

A kockázatok kezelése az alábbi módon történhet:
- elfogadással
- enyhítéssel
- elkerüléssel
- átruházással -kivéve az érintettek jogait és szabadságait érintő kockázatok

A kockázatkezelési döntéseket minden esetben írásban rögzíteni kell.
A kockázatenyhítési kezdeményezéseket valós időben, indoklással kell meghatározni.
Az ezekből elindított kockázatcsökkentő projekteknek egyértelmű utasításokat kell tartalmazniuk, meghatározva a projekt felelőseit, határidejét, hogy a kockázatot megfelelő módon csökkentsék.

VI. AZ INFOKOMMUNIKÁCIÓS RENDSZER FELÉPÍTÉSE

VI.1. Szerverek

A **Foster Kft** minden adatát szerverek tárolják. melyek a informatikai hálózathoz csatlakoztatva biztosítják az adatok megfelelő elérését helyi illetve internetes felületen. Internetkapcsolaton VPN segítségével bárhonnan elérhető, a tárolt adatok megoszthatók, védhetők a felhasználói engedélyek beállításával.

A **Foster Kft.** valamennyi telephelyén üzembe helyezett Tűzfal az alábbi funkciókat biztosítja:

- Fájlok kezelése és elérése
- VPN szerver: A VPN Server lehetővé teszi, hogy a L2TP/IPSec VPN (virtuális magánhálózati) kapcsolatot létesíthessen vele a Felhasználó és a helyi hálózaton megosztott erőforrásainak elérését.
- Adatforgalom monitorozása és szűrése

A szerverek minden adata és alkalmazása rendszergazda által meghatározott biztonságos belépéssel és jogosultsági szinteken érhető el. Ezeket dokumentálni kell.

VI.2. Infokommunikációs hálózat, vezeték nélküli hálózat

A **Foster Kft.** székhelyén, az egyes telephelyein a rendelkezésre álló Internet eléréseket egy tűzfal eszköz és hozzá kapcsolat switch-en keresztül érik el a **Felhasználók**. A telephelyeken rendelkezésre állnak vezeték nélküli hálózat kiszolgálására hozzáférési pontok is.

A vezeték nélküli hálózatok elérése WPA2-PSK (AES) protokoll szerinti védett módon történik.
Minden telephelyén és ügyfélszolgálatán rendelkezésre áll egy úgynevezett vendég vezeték nélküli hálózat is, mely a helyiségben kifüggesztett jelszóval védett és VLAN-nal el van szeparálva a belső hálózattól.

A mobil eszközök telephelyen kívüli használatakor a **Foster Kft.**-hez történő csatlakozás szoftveres VPN-en keresztül történik.

VI.3. Kliens gépek

A kliens számítógépek- melyekbe beletartoznak az alvállalkozók által használt gépek is- Microsoft Windows operációs rendszerrel üzemelnek. A helyi hálózathoz az adottságoknak megfelelően vagy kábelen, vagy biztonságos vezeték nélküli hálózaton csatlakoznak.
Minden kliens gép rendelkezik önálló vírusvédelemmel valamint TPM titkosító chippel.
A kliens gépeken a **Foster Kft**. felhasználói rendszergazdai jogosultsággal nem rendelkeznek, minden rendszergazdai jogosultságot igénylő feladatot a rendszergazda engedélyével az azzal megbízott személy a helyi, vagy távoli hozzáféréssel, ideértve az egyes új hardverelemek csatlakoztatását, alkalmazások telepítését is.

VI.4. Adatmentés

Az szerveren tárolt adatok RAID-be szervezett HDD-ken tárolják az adatokat, ami egy HDD meghibásodása esetén nem okoz adatvesztést a **Foster Kft.** számára. Ezen túl az adatok a **Foster Kft** backup szerverén is mentésre kerülnek napi és heti rendszerességgel.

VI.5. Adat-visszaállítás

Az adatmentések, adat szinkronizációk ellenőrzése: a rendszergazda által legalább hetente ellenőrzésre kerülnek, valamint ellenőrzés céljából havi rendszerességgel történnek részleges adat-visszaállítások.

Az adat-visszaállítás menete:

- Az adat-visszaállítás igényét, a visszaállítandó állományok pontos meghatározásával az érintett könyvtár adatgazdája jelzi a rendszergazda felé
- A rendszergazda ellenőrzi a kérés jogosságát a jogosultságok lista alapján, a további lépéseket csak a jogos kérés esetén hajtja végre.
- A rendszergazda másolatot készít a szerveren esetlegesen felülírásra kerülő állományokról.
- A rendszergazda kiválasztja a visszaállítandó állományokat a backup szerveren.
- A rendszergazda átmásolja a kért állományokat az backup szerverről az éles szerverre.
- A rendszergazda tájékoztatja az adatgazdát az adat-visszaállítás tényéről (ki, mikor, mit végzett).

VII. INFOKOMMUNIKÁCIÓS FOLYAMATOK

VII.1. Munkaviszony vagy munkavégzésre irányuló alvállalkozói jogviszony létesítéséhez kapcsolódó infokommunikációs folyamat

Közvetlen vezetői tájékoztatás	Munkaviszony létesítése esetén az ügyvezető igazgató, munkavégzésre irányuló alvállalkozói jogviszony létesítése esetén a jogviszony létesítését kezdeményező ügyvezető a jogosultsági igény időpontja előtt fő szabály szerint 3 munkanappal, rendkívüli esetekben haladéktalanul tájékoztatja a belépő a szakmai vezetőt és a titkárságvezetőt a belépésről.
Az infokommunikációs igény meghatározása	Felelős: ügyvezető igazgató
Igény jóváhagyása	Felelős: ügyvezető igazgató
A nem szabványos, igények külön engedélyezése	Felelős: Ügyvezető titkárságvezető,
Jelen Szabályzat megismertetése és elfogadtatása az 1. számú mellékletben szereplő Informatikai felhasználói nyilatkozat aláíratásával.	Felelős: Ügyvezető, szakmai vezető
Új eszköz használata előtt az eszköz használatára vonatkozó képzés	Felelős: rendszergazda, szakmai vezető
Az igényelt eszközök előkészítése és a felhasználónak történő átadása.	Felelős: Szakmai vezető A Szakmai vezető a leendő Felhasználó részére átadandó eszközökről, átadás-átvételi megállapodást készít a 2. számú melléklet alapján; a nem aktivált eszközök esetében elkészíti az üzembe helyezési dokumentumokat.

Könyvelés elvégzése	Felelős: gazdaság vezető

VII.2. Munkaviszony vagy alvállalkozói jogviszony megszűnéséhez kapcsolódó infokommunikációs folyamat

ügyvezető igazgató tájékoztatása	Munkaviszony megszűnése esetén a ügyvezető igazgató j munkavégzésre alvállalkozói egyéb jogviszony megszűnése esetén az ügyvezető igazgató a jogviszonyok megszűnése időpontja előtt fő szabály szerint 3 munkanappal, rendkívüli esetekben haladéktalanul tájékoztatja a rendszergazdát és az adatvédelmi biztost a jogviszony megszűnéséről. Ezt követően történik meg valamennyi elektronikus „aláírás/jóváhagyást" követően a kiléptetés, illetve végső elszámolás.
A jogosultságok visszavonása, és az eszközök visszavétele, az intézkedés végrehajtásáról a kezdeményező tájékoztatása	Felelős: rendszergazda
Könyvelések elvégzése	Felelős: gazdasági vezető

VII.3. Infokommunikációs eszköz, szoftver visszaszolgáltatása

az ügyvezető tájékoztatása az eszköz vagy szoftver használatának megszűnéséről	Felelős: érintett ügyvezető igazgató
A jogosultságok visszavonása, és intézkedés az eszközök visszavételéről.	Felelős: rendszergazda, szakmai vezető
könyvelések elvégzése	Felelős: gazdasági vezető

VII.4. Infokommunikációs incidens kezelése

Rendszergazda haladéktalan tájékoztatása az eszköz vagy szoftver használatának megszűnéséről	Felelős: Felhasználó
Intézkedés az incidens megoldásáról az incidens prioritásának és a javítás módjának megfelelően telefonon, távfelügyelettel, vagy helyszíni megjelenéssel, és a megoldásról visszajelzést ad az érintetteknek. A rendszergazda naplót vezet az összes bejelentett incidensről, azok hatásáról és kezeléséről.	Felelős: rendszergazda, adatvédelmi biztos
Valamennyi, az adatokat, dokumentumokat érintő biztonsági incidenst haladéktalanul jelenteni kell az adatgazdának	Felelős: Felhasználó, rendszergazda, adatvédelmi biztos
Amennyiben az incidens megoldása költséggel jár, abban az esetben az "Infokommunikációs eszköz, szoftver igénylése" folyamat indítása megfelelő indoklással	Felelős: rendszergazda, adatvédelmi biztos, ügyvezető igazgató

VIII. INFOKOMMUNIKÁCIÓS BIZTONSÁG

VIII.1. Eszközök használata

A **Foster Kft.** és alvállalkozóinak infokommunikációs eszközei kizárólag a **Foster Kft.** üzleti céljaira használhatók, az infokommunikációs eszközök magáncélú használata tilos.

VIII.2. Az eszközök fizikai védelme

- Tilos az eszközök közelében élelmiszert, italt fogyasztani, dohányozni.
- Tilos a szerverterem teljes területén élelmiszert fogyasztani, vagy azokat kicsomagolt állapotban tartani.
- Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.
- A **Felhasználók** kötelesek minden meghibásodást jelenteni a rendszergazda részére.
- A **Felhasználóknak** tilos az eszközök elektromos csatlakozásait megbontani. Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt áramtalanítani kell. Ha a meghibásodás nem elszigetelhető, hanem a helyiség teljes elektromos hálózatában keletkezik, úgy az egész helyiséget áramtalanítani kell a főkapcsolóval.
- Az eszközök használatát az ügyvezető igazgató által arra kijelölt személy ismerteti, akinek feladata az eszközök kezelésének bemutatása, az ahhoz kapcsolódó speciális tudnivalók ismertetése. Minden Felhasználó csak azokat az eszközöket használhatja, amelyekre engedélyt kapott, és kezelésükre ki lett oktatva. A használható eszközök körének meghatározása a felhasználói jogosultság kiadásával párhuzamosan történik.
- Tartalék berendezést, mentést tartalmazó adathordozót/eszközt úgy kell elhelyezni, hogy az eredeti berendezést/adattárat érintő esetlege külső hatástól lehetőség szerint mentes legyen.
- Tilos a kábelezést a fali csatlakozónál megbontani, és közvetlenül a kábelre gépet csatlakoztatni. A fali csatlakozó és a számítógép között lengőkábelt kell használni.
- Tilos a Foster Kft. belső hálózatára idegen eszközt csatlakoztatni.
- A hálózathoz való csatlakozáshoz szükséges címek felett a Foster Kft. rendelkezik. Tilos önkényesen címeket megadni, vagy megváltoztatni. Szükség esetén a Foster Kft. jogosult a már kiadott címek visszavonására vagy megváltoztatására.

VIII.3. Az eszközök környezetének védelme

Infokommunikációs eszközöket csak olyan területeken lehet elhelyezni, ahol azokat az illetéktelenektől határzóna, vagy elzárási lehetőség védi.

VIII.4. Az eszközök tulajdonának védelme

Alkalmazás megszűnés esetén az eszközöket a munkavállalóktól leltár szerint vissza kell venni. A **Felhasználó** felelős, hogy az általa átvett eszközt az átvételnek megfelelő állapotban adja vissza.

Mind a munkavállalók mind az alvállalkozók esetén a karbantartásra/selejtezésre kivitt eszközök esetén a rendszergazdának biztosítani kell, hogy az eszközön ne legyenek visszaállítható adatok. Eszközök áthelyezése során azok adatokat csak a szükséges mértékben tartalmazhatnak.

VIII.5. Jelszóhasználat

A **Felhasználó** felelős, hogy a jelszavát titkosan kezelje.
Amennyiben az infokommunikációs rendszerek jelszót igényelnek, ún. erős jelszót kell alkalmazni, melynek kritériumai az alábbiak:

- legalább 6 karakter hosszúságú
- vegyesen tartalmaz kis- és nagybetűket, számokat és szimbólumokat
- legalább kéthavonta meg kell változtatni
- az új jelszónak az azt megelőző két jelszótól eltérőnek kell lennie
- szótárak nem tartalmazhatják, nem lehet szótári alak
- nem tartalmazza a **Felhasználó** családi nevét, felhasználónevét, sem egyéb **Felhasználóhoz** kapcsolódó információt

VIII.6. Jogosultságkezelés

Munkavégzésre irányuló jogviszony létesítés, illetve munkakör váltás miatti jogosultságváltozás, valamint a munkavégzésre irányuló jogviszony megszűnése esetén az ügyvezető igazgató a jogosultságváltozás időpontja előtt fő szabály szerint 3 munkanappal, rendkívüli esetekben haladéktalanul elindítja a jogosultságváltozás és az infokommunikációs eszköz igénylés dokumentált folyamatát.

VIII.7. Vírusvédelem

A levelezési rendszert külön naponta frissített vírusirtó védi.
A szervereket központi, naponta frissülő vírusirtó védi.
A számítógépeken vírusirtó és behatolás védő szoftver van. A központi rendszerre kapcsolódva a központi vírusirtó is aktiválódik.
A központi rendszert a külső behatolások ellen a rendszergazda által folyamatosan frissített tűzfal védi. A forgalmat a rendszergazda folyamatosan ellenőrzi.

VIII.8. Szoftverek telepítése

Tilos a nem engedélyezett szoftverek, filmek, zenék és más szerzői jogvédelem alá eső anyagok másolása, letöltése. Szoftvert csak rendszergazda, illetve a rendszergazda jóváhagyásával a ügyvezető által megnevezett szakmai munkatárs telepíthet.

VIII.9. Infokommunikációs incidens

A **Felhasználónak** az infokommunikációs rendszer meghibásodása esetén haladéktalanul értesítenie kell az adatkezelési megbízottat és a rendszergazdát. Valamennyi, az adatokat, dokumentumokat érintő biztonsági incidenst haladéktalanul jelenteni kell az adatgazdának is.

VIII.10. E-mail és internet használat

A **Foster Kft.** e-mail címei kizárólagosan a társaság üzleti levelezésére használhatók. Fájlok letöltése az Internetről nem engedélyezett, kivéve, ha ellenőrzött forrásból származnak, és a **Foster Kft.** üzleti céljaira szükségesek. A fájlok letöltése során a **Felhasználó** személyes felelősséggel tartozik, hogy megbizonyosodjon a forrás hitelességéről. Bizonytalanság esetén a **Felhasználó** kérheti a rendszergazda segítségét, hogy ellenőrizze a letölteni kívánt fájlokat.

VIII.11. Adat és dokumentum tárolás

A számítógépeken ún. kritikus adatok (személyes, valamint a Foster Kft. működésére vonatkozó), állományok csak átmenetileg tárolhatók. A szükséges feladatok elvégzése után az adatokat a hálózatra kell menteni.

VIII.12. Mobil eszközök

A **Felhasználó**nak gondoskodni kell, hogy tulajdonában lévő mobil eszközök („okos telefonok", tabletek, laptopok) az elvárt funkcionalitással rendelkezzenek. Abban az esetben, ha az „okos telefonon” a Foster Kft. tulajdonát képező adatok és dokumentumok tárolása történik, az eszközt olyan jelszóvédelemmel kell ellátni, amely egy meghatározott idő elteltével lezárja az eszközt.

Békéscsaba, 2019. január 31.

Fazekas István
ügyvezető igazgató

1. számú melléklet

Informatikai felhasználói nyilatkozat

Alulírott _____ (a továbbiakban Felhasználó) (anyja neve: _____lakóhely: _____) a jelen nyilatkozat aláírásával kijelentem, hogy:

- a **FOSTER Biztosítási Alkusz Kft.** (a továbbiakban: **Foster Kft**.) **Informatikai üzemeltetési és informatikai biztonsági Szabályzatát** (a továbbiakban: **Szabályzat**) megismertem, annak tartalmát megértettem, rendelkezéseit magamra kötelezőnek ismerem el, és mint **Felhasználó**, elfogadom;
- az Foster Kft. adatkezelési rendszerét, beleértve a részemre rendelkezésre bocsátott számítástechnikai infrastruktúrát, számítógépes hálózatot, csak a **Szabályza**t elfogadásával és betartásával használom,
- minden olyan kár és esemény miatt, amelyet a **Szabályzat** vagy a jogszabályok általam történő megszegése okoz, teljes anyagi és büntetőjogi felelősséggel tartozom, ideértve az alábbi eseteket is:
    - ha a Foster Kft. hálózatán vírusfertőzés,
    - adatvesztés történik,
    - vagy adatok illetéktelenek számára való hozzáférése válik lehetővé.

A továbbiakban nyilatkozom, hogy tudomásul veszem és elfogadom, hogy:

- a **Foster Kft**. infokommunikációs eszközei kizárólag az **Foster Kft.** üzleti céljaira használhatók, az infokommunikációs eszközök magáncélú használata tilos;
- a **Foster Kft**. jogosult a Felhasználók rendelkezésére bocsátott számítástechnikai infrastruktúrába tartozó eszközök ellenőrzésére;
- a szerzői jog által védett számítógépes szoftverek, média és egyéb állományok jogtalan használata és másolása törvénybe ütköző cselekedet;
- a **Foster Kft.** infokommunikációs rendszerén kizárólag a **Foster Kft**. által biztosított szoftvereket használhatom, ideértve a licence köteles vagy szabad szoftvereket is;
- minden egyedi igény és jogosultság-módosítási kérelmet a **Szabályzatban** foglaltak szerint kell jelezni;
- az a **Felhasználó**, aki a Foster Kft. által biztosított infokommunikációs eszközein illegális szoftvert, vagy a szoftver telepítéséhez szükséges állományt tárol, bűncselekményt követ el, valamint ha a **Szabályzat** megszegésével megszerzett szoftvert, adatot, szoftver telepítéséhez szükséges állományt tárol kötelezettségszegést követ el.

Budapest, 201... év ..... hónap……..nap

_____

Aláírás

2. számú melléklet

Átadás-átvételi megállapodás

_____ (a továbbiakban Átvevő) (anyja neve: _____lakóhely: _____) a mai napon használatra átvette a FOSTER Biztosítási Alkusz Kft. (a továbbiakban: **Foster Kft**.) alábbi eszközeit:

Eszköz/tartozék megnevezése	**Gyári azonosító**	**Leltári szám**	**Egyéb azonosító**

Átvevő kötelezettséget vállal az alábbiakra:

- Az adott helyzetben általában elvárható legnagyobb gondossággal kezeli, használja az eszközöket és az azon tárolt üzleti adatokat.
- A **Foster Kft**. székhelyén, telephelyén kívül az eszközöket nem tartja parkoló autóban, illetve nem tárolja nyilvános helyen őrizetlenül.
- Átvevőt az átvett eszközök elvesztése, megrongálódása, egyéb károsodása tekintetében kártérítési felelősség terheli.
- Amennyiben a **Foster Kft**.-n kívül kapcsolódik az internethez (pl. hotelben vagy otthoni ADSL), akkor meggyőződik arról, hogy az adott hálózat tűzfallal (firewall) védett.
- Az eszköz otthoni használata során is betartja a **Foster Kft**. **Informatikai üzemeltetési és informatikai biztonsági Szabályzatában** foglalt előírásokat.

Kelt _____ , 20 _____

_____ _____

Átadó
Foster Kft. részéről

Átvevő