Comnica Kft.
Bizalmi Szolgáltatási Szabályzat

Elektronikus aláírás elhelyezése

CÍM: Comnica Kft. Bizalmi Szolgáltatási Szabályzat

HATÁLYA: Jelen szabályzat 2022.12.01-től lép hatályba
FELÜLVIZSGÁLAT: Kötelező felülvizsgálat 2023.12.01 előtt

ELFOGADVA:

Név	Beosztás	Dátum	Aláírás

ÁTTEKINTVE:

Név	Beosztás	Dátum	Aláírás

A dokumentum aláírás nélkül is érvényes.

Tartalom

Dokumentum történet

OID	Verzió	Hatálybalépés dátuma	Változás / Megjegyzés
COM_H0075	1	2022.12.01.	Dokumentum létrehozása

1. Általános rész

1.1. A szabályzat célja

Jelen Bizalmi Szolgáltatási Szabályzat (továbbiakban: BSzSz) célja, hogy:

- A Comnica Kft. (továbbiakban: „Szolgáltató") - nem minősített bizalmi szolgáltató vonatkozásában - e keretszabályzatban rögzítse a bizalmi szolgáltatásokhoz kapcsolódó adat- és információbiztonság feltételeit, környezetét.
- Szabályozza a Szolgáltató tulajdonában lévő, illetve az általa üzemeltetett bizalmi szolgáltatásokhoz kapcsolódó informatikai rendszerek által kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását és funkcionalitását az azokat fenyegető veszélyekkel szemben társasági szinten, általános jelleggel.
- Elősegítse a Szolgáltató megfelelését a bizalmi szolgáltatásokhoz kapcsolódó törvényi rendelkezéseknek.

2. A szabályzat hatálya

Jelen szabályzat időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Módosítások esetén a Szolgáltató a módosítást megelőzően 30 nappal közzéteszi a honlapján a módosított szabályzatot, illetve tájékoztatja a bizalmi felügyeletet. Az új verzió hatályba lépésével a korábbi verzió rendelkezései megszűnnek.

2.1. A BSzSz személyi hatálya

A BSzSz személyi hatálya kiterjed a Szolgáltató valamennyi (fő-, rész-, másod- és mellékfoglalkozású) munkavállalójára. Továbbá kiterjed azon személyekre, akik a Szolgáltatóval munkavégzésre irányuló egyéb jogviszonyban állnak, ideértve a Szolgáltató részére megbízási szerződés alapján munkát végző személyeket is.

2.2. A BSzSz tárgyi hatálya

A BSzSz tárgyi hatálya kiterjed a Szolgáltató tulajdonában lévő vagy az általa üzemeltetett valamennyi meglévő és a jövőben fejlesztendő informatikai rendszerre, illetve azok környezetét alkotó rendszerelemekre, azok teljes életciklusában (az előkészítéstől a rendszerből történő kivonásig), az információfeldolgozás teljes folyamatára, életciklusára.

2.3. A BSzSz területi hatálya

A BSzSz területi hatálya kiterjed a Szolgáltatóra, illetve a tulajdonában lévő vagy az általa bérelt épületekre, helyiségekre, telephelyekre.

3. A BSzSz elérhetősége

A BSzSz aktuális verziója elérhető a Szolgáltató honlapján: www.comnica.com

4. A karbantartásért, elkészítésért felelős szervezeti egység

A dokumentumot évente minimum egyszer felül kell vizsgálni.
A dokumentumot frissíteni szükséges minden olyan esetben, amikor az üzleti célok vagy a kockázati környezet jelentősen módosul.

5. Kapcsolódó dokumentumok, szabályzatok, utasítások

- Bizalmi Szolgáltatási Rend (nyilvános)
- Bizalmi Szolgáltatási Szerződés

- Adatkezelési tájékoztató
- Panaszkezelési szabályzat

6. Fogalmak és meghatározások

Adat:
Az információ megjelenési formája, értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) ismeret.

Adatbiztonság:
Az adatokhoz történő jogosulatlan hozzáférés, az adatok módosítása és tönkretétele elleni műszaki és szervezési intézkedések, illetve eljárások együttes rendszere.

Bizalmi munkakör:
- A szolgáltató informatikai rendszeréért általánosan felelős vezetői munkakör,
- biztonsági tisztviselő munkakör: a szolgáltatás biztonságáért általánosan felelős személy munkaköre,
- rendszeradminisztrátori munkakör: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy munkaköre,
- rendszerüzemeltető munkakör: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy munkaköre,
- független rendszervizsgálói munkakör: a Szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a Szolgáltató által a szabályszerű működés érdekében megvalósított kontrollintézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy munkaköre.

Bizalmi szolgáltatást megvalósító termék:
A belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet (a továbbiakban: eIDAS Rendelet) 3. cikk 21. pontja szerinti termék.

Információbiztonsági irányítási rendszer:
A Szolgáltatónál az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése érdekében működtetett irányítási rendszer.

Informatikai rendszer:
A Szolgáltató által a bizalmi szolgáltatásokhoz, illetve annak elemeihez, valamit a bizalmi szolgáltatói tevékenységek informatikai védelméhez használt, az eIDAS Rendelet 24. cikk (2) bekezdés e) és f) pontja szerinti megbízható rendszerek és termékek együttese (v. halmaza, összessége).

Kriptográfiai kulcs:
Olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás vagy bélyegző előállításához vagy ellenőrzéséhez szükséges.

Minőségirányítási rendszer:
A Szolgáltatónál a minőségbiztosítás érdekében működtetett irányítási rendszer.

Partner:
A Szolgáltatóval ügyfélazonosítás és elektronikus aláírás elhelyezésére vonatkozóan szerződéses viszonyban lévő olyan gazdasági társaság vagy szervezet, amely meglévő vagy leendő ügyfelei vonatkozásában végez ügyfélazonosítást, illetve online szerződéskötést.

Rendkívüli üzemeltetési helyzet:

Olyan, a Szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amelyben a Szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség. Rendkívüli üzemeltetési helyzetnek minősül az is, ha a Szolgáltató szolgáltatói magánkulcsa olyan személy birtokába kerül, aki a szolgáltatói magánkulcs birtoklására nincsen feljogosítva, illetve, ha a fenti esemény megtörténte alappal feltételezhető vagy annak közvetlen veszélye fennáll.

Szolgáltató:
A Comnica Kft., az E-ügyintézési tv. szerinti bizalmi szolgáltató.

Szolgáltatói kulcspár:
A szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs.

Szolgáltatói magánkulcs:
Olyan kriptográfiai kulcs, amelyet a Szolgáltató saját bizalmi szolgáltatásának igazolására, így különösen az időbélyegzésre, a naplózáshoz és az archiváláshoz használ.

Szolgáltatói nyilvános kulcs:
Olyan kriptográfiai kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak.

Ügyfél:
A Szolgáltató Partnerével üzleti kapcsolatban lévő természetes személy vagy gazdasági társaság, aki a Szolgáltató azonosítási szolgáltatását követően igénybe veszi a jelen Bizalmi Szolgáltatási Szabályzat kereteinek megfelelően működő aláíró modult.

Változáskezelés:
Azon szabályok összessége, amelyek meghatározzák a szolgáltatási folyamatokban és az azt kiszolgáló informatikai szolgáltatásokban bekövetkező módosítások, változások biztonságos végrehajtását.

7. A Bizalmi Szolgáltatás

7.1. Kapcsolati adatok

Cégnév: **Comnica Kft.**
Adószám: **14242036-2-43**
Cégjegyzékszám: **01-09-895207**
Székhely: **1119 Budapest, Mohai út 38.**
Weboldal: **www.comnica.com**

7.2. A Comnica Kft. által nyújtott bizalmi szolgáltatások

A Szolgáltató az eIDAS rendelet 3. cikk 16.a) pontja szerinti elektronikus aláírás elhelyezését végzi, mely az alábbi követelmények alapján fokozott biztonságú elektronikus aláírásnak minősül:

- kizárólag az aláíróhoz köthető,
- alkalmas az aláíró azonosítására,
- olyan adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat,
- az aláírást követően a dokumentum létrehozásának időpontja és az azóta történt változatlansága ellenőrizhető.

7.3. A bizalmi szolgáltatás díjazása

A Szolgáltató a jelen szabályzatban foglalt bizalmi szolgáltatást, melyben a személy azonosítását követően az Ügyfél nyilatkozatának megfelelően az Ügyfél által elfogadott dokumentumon elektronikus aláírást helyez el, az Ügyfelek számára díjmentesen végzi.

7.4. Felügyeleti szervek

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: „NMHH”).
A jelen BSzSz-ben foglalt szolgáltatás (Elektronikus aláírás elhelyezése) 2022.10.28-án került bejelentésre az NMHH részére.
Az NMHH elérhetősége: www.nmhh.hu

7.5. Panaszkezelés, ügyfélszolgálat

A vitáikat a felek mindenkor megkísérlik békés úton, tárgyalások útján rendezni. A jelen Szabályzatban meghatározott Szolgáltatással összefüggő panasz vagy jogvita esetén lehetőség van a Békéltető Testülethez vagy az illetékes bírósághoz fordulni.

A Szolgáltató Panaszkezelési Szabályzata elérhető az alábbi weboldalon: www.comnica.com

A Békéltető Testület elérhetőségei az alábbi weboldalon érhetőek el: https://bekeltet.bkik.hu/elerhetosegek

7.6. Adatszolgáltatás, módosítás

A Szolgáltató számítógépes rendszere alkalmas azok rendszerelemeinek a jogszabályban és a belső szabályokban előírt módon történő rendszerszintű összekapcsolására, illetve biztonságos és megbízható szolgáltatások nyújtására, amely magában foglalja a tevékenységből eredő adatszolgáltatási és módosítási kötelezettséget is.
A Szolgáltató biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

A BSzSz módosulását minden esetben a verziószám megfelelő változása követi. A Szolgáltató minden módosítást 30 nappal a változást megelőzően elérhetővé tesz honlapján. A Szolgáltató minden változtatást a a belső szabályzataival összhangban végez és folyamatosan ellenőrzi a bizalmi szolgáltatásra vonatkozó ÁSZF, BSzSz és a

Bizalmi Szolgáltatói Rend összhangját.

7.7. Törvényi háttér

A Szolgáltató mindenkor a magyar és az Európai Unió jogszabályainak megfelelően végzi tevékenységét, különös tekintettel az alábbi jogszabályokra, rendeletekre:

- 1996. évi LVII. törvény
- 2013. évi V. törvény (továbbiakban: Ptk.)
- 2011. évi CXII. törvény
- 910/2014/EU EP rendelet (továbbiakban: eIDAS)
- 2015. évi CCXXII. törvény (továbbiakban: E-ügyintézési tv.)
- 24/2016 (VI. 30.) és 25/2016 (VI. 30) BM rendelet
- 470/2017. (XII. 28.) és a 137/2016 (VI. 13.) Kormányrendelet

A Szolgáltató nem felel jelen szerződésben megállapított valamely kötelezettsége teljesítéséért azokban az esetekben, amikor olyan, bármely fél érdekkörén kívül eső, előre nem látható, illetve elháríthatatlan körülmények (vis major) merülnek fel, amelyek megakadályozzák a szolgáltatás teljesítését. Ilyen körülmények különösen, de nem kizárólagosan: háborús cselekmények, lázadás, szabotázs, robbantásos merénylet, szükséghelyzet, elemi csapás (árvíz, tűzvész, villámcsapás, szél- és hóvihar, belvíz, más természeti katasztrófa, közműszolgáltatás szünetelése), illetve a törvény alapján arra feljogosított szervezetek rendkívüli helyzetben tett intézkedéseinek következményei, melyek a szerződő feleket a szerződésben vállalt kötelezettségeik teljesítésében korlátozzák vagy gátolják és ennek eredményeként vétlen módon vagyoni vagy nem vagyoni kárt okoznak.

7.8. Felelősség és felelősségbiztosítás

Felelősség:
A Szolgáltató köteles jelen szabályzatban és az egyéb bizalmi szolgáltatáshoz kapcsolódó dokumentumban megfogalmazott feltételeknek mindenkor megfelelni. A szabályzatoknak történő megfelelés abban az esetben is érvényes, amikor egyes tevékenységeket a Szolgáltató kiszervez.

Felelősségbiztosítás:
A Szolgáltató rendelkezik olyan felelősségbiztosítással, amely kiterjed a bizalmi szolgáltatással összefüggésben okozott károkra és költségekre. A Szolgáltató vállalja, hogy a felelősségbiztosítás biztosítási összege mindenkor legalább 5.000.000 Ft.

A felelősségbiztosítás kiterjed a Szolgáltató által nyújtott bizalmi szolgáltatásokkal összefüggésben okozott alábbi károkra és költségekre:

- a bizalmi szolgáltatást igénybe vevő Ügyfélnek a bizalmi szolgáltatási szerződés megszegésével összefüggésben okozott károkra,
- a bizalmi szolgáltatást igénybe vevő Ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- az E-ügyintézési tv. 88. §-ában foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az E-ügyintézési tv. 89. §-a szerinti költségekre és
- az eIDAS Rendelet 17. cikk (4) bekezdés e) pontja alapján a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

8. A bizalmi szolgáltatások folyamatai

8.1. Azonosítás és elektronikus aláírás elhelyezése

A Szolgáltató az eIDAS rendeletnek megfelelően egy PDF fájlra az Ügyfél azonosítása után az Ügyfél nevében elektronikus aláírást helyez el. Az aláírás elhelyezése után a dokumentum tartalma megváltoztathatatlan, letagadhatatlan és az aláírás egyértelműen visszavezethető az aláíró személyre.

Azonosítás

Az aláírás elhelyezéséhez szükséges feltétel az aláíró személy előzetes azonosítása. Ezt az azonosítást a Partner végzi a Szolgáltató által fejlesztett és SaaS módon biztosított azonosítási rendszerben. Az azonosítás során a Partner a vonatkozó jogszabályi kereteknek megfelelően elvégzi az Ügyfél azonosítását, bekéri és kezeli a személyes adatait. Kizárólag sikeres azonosítást követően van lehetőség az elektronikus aláírás elhelyezésére. Az aláírási folyamat elindításához az aláíró modul részére át kell adni az Ügyfél azonosítás során ellenőrzött adatait (név, e-mail cím, telefonszám) és egy egyedi azonosítót, mellyel az azonosítási ügy bármikor a jövőben visszakövethető, annak tartalma (okmányfotók, videók, keletkezett adatok) a Szolgáltató és a Partner számára megismerhető. Ezen adatok felhasználásával készül el a folyamat későbbi részeiben az elektronikus aláírás.

Az aláírási folyamat elindítása

Az aláírás elindításához a következő adatoknak kell rendelkezésre állnia:

- Az azonosítás során ellenőrzött személyes adatok: név, e-mail cím, telefonszám, azonosítási ügyazonosító.
- A Partner által előkészített dokumentumok pdf formátumban.
- Az aláírás esetleges határideje.

Amint a fenti adatok rendelkezésre állnak, az aláírás az Ügyfél ellenőrzött e-mail címére küldött egyedi URL segítségével indítható. A rendszer ellenőrzi az egyedi URL-ben található ügyféltoken érvényességét és egy második faktoros authentikáció után - az Ügyfél azonosítása során ellenőrzött telefonszámra küldött SMS segítségével - az Ügyfél elvégezheti az aláírandó dokumentumok átnézését.
Miután a dokumentumokat az Ügyfél átolvasta, ellenőrizte, azok tartalmát megismerte, az aláíráshoz a rendszer erre biztosított felületén elfogadja a dokumentumokat és kezdeményezi az aláírás elhelyezését.

Az aláírás elhelyezése

A rendszer a Comnica Minősített Tanúsítványa segítségével a PDF dokumentumra elektronikus aláírást és minősített időbélyegzőt helyez el RSA algoritmussal. A dokumentumot a Comnica tanúsítványához tartozó titkos kulcs segítségével aláírja, majd a későbbi ellenőrizhetőséghez a kulcs publikus párját és a tanúsítványát belefoglalja a PDF fájlba.
A Szolgáltató az aláírás időpontjának igazolásához Hiteles Időbélyeg Szolgáltatótól származó időbélyeget helyez a dokumentumba. A hosszú távú ellenőrizhetőség (LTV) érdekében az online tanúsítvány-állapot szolgáltatástól (OCSP) kapott választ is csatolja az aláíráshoz, a PAdES előírásainak megfelelően. Az aláírásnak vizuális megjelenítése a dokumentumban nincs, csak a PDF objektum aláírásmezőit használja fel. Az aláíráshoz a Szolgáltató jelen dokumentum készítésekor SHA-512 hash algoritmust használ, de figyelemmel követi ezen algoritmusok biztonságosságát. Az aláírás Name mezőjébe belefoglalja az Ügyfél nevét, a Reason mezőjébe pedig belefoglalja az azonosítás egyedi azonosítóját, melynek segítségével az aláíró személy a jövőben bármikor a Comnica mint Bizalmi Szolgáltató vagy a Partner segítségével ellenőrizhető. Ezzel a módszerrel a PDF fájlra több aláírást is el lehet helyezni.

Az aláírás ellenőrzése

Az aláírás ellenőrzéséhez bármilyen, PDF aláírást támogató program (pl. Adobe Reader, PDFsig) vagy online szolgáltatás (pl. https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation) szükséges. Ezekben az eszközökben az aláírás fülön egyszerűen ellenőrizhető a tanúsítvány hitelessége és az aláíró neve. Amennyiben szükségessé válik - egy esetleges jogvita esetén - az aláíró további személyes adatainak megismerése, úgy az aláírásban foglalt azonosítási ügyazonosító segítségével a Szolgáltató bármikor ellenőrizni tudja az Ügyfél azonosításkor bemutatott személyes adatait, arcképét, okmányfotóit.

8.2. Szolgáltatói kulcsok kezelése

A Szolgáltató az ügyféllel való kapcsolattartás során nem bocsát ki tanúsítványt. Ennek okán a Szolgáltató nem tesz közzé tanúsítványokkal kapcsolatos információt, beleértve a szolgáltatói kulcsokkal kapcsolatos információkat sem.

9. Szervezeti biztonság

9.1. Az informatikai biztonság szervezeti struktúrája

Az informatikai biztonság megtervezését, megvalósítását és ellenőrzését a Szolgáltató szervezeti hierarchiáján alapuló rendszer biztosítja.
Az informatikai biztonságnak a törvényekben és más jogszabályokban, a Szolgáltató szerződéseiben és megállapodásaiban, valamint az ügyviteli és a jelen szabályzatban előírt elvárások megvalósításáért valamennyi érintett szervezeti egység vezetője felelős.

9.2. Az informatikai biztonság intézményrendszere

A Szolgáltató folyamatosan biztosítja, hogy a bizalmi szolgáltatás vonatkozásában a kontrollrendszer működtetéséhez megfelelő képzettséggel és ismeretekkel rendelkező, megfelelő számú - a Szolgáltatóval munkaviszonyban lévő - személyzet áll rendelkezésre. A bizalmi szolgáltatás vonatkozásában az alábbi alapvető szerepkörökre mindenkor kijelölésre kerülnek az elsődleges és a helyettesítő személyek, melyekről a Szolgáltató nyilvántartást vezet:

- Biztonsági tisztviselő
- Informatikai vezető
- Független rendszervizsgáló
- Üzemeltető, rendszergazda
- Rendszer-adminisztrátor

9.3. Feladatkörök szétválasztása

A Szolgáltató a 24/2016 BM. rendelet 4.§-ban foglaltaknak megfelelően folyamatosan biztosítja, hogy a biztonsági tisztviselő ne láthassa el a független rendszervizsgáló és az informatikai rendszerért általánosan felelős vezető feladatait és a független rendszervizsgáló ne láthassa el az informatikai rendszerért általánosan felelős vezető feladatait.

9.4. Oktatás

Biztonságtudatossági oktatás

A Szolgáltató mindenkor biztosítja, hogy a bizalmi szolgáltatás nyújtásához megfelelő létszámú, képzettségű, szakmai gyakorlattal és tudással rendelkező személy álljon rendelkezésre. A Szolgáltató rendszeresen képzéseket tart annak érdekében, hogy a rendszerek működtetése során a szoftverek és a fizikai eszközök működése üzemszerűen és biztonságosan történjen.
A Szolgáltató kiemelt figyelmet fordít arra, hogy a rendszerben történő jelentősebb változásokat megelőzően a munkatársak megkapják a változtatásokra vonatkozó képzést, illetve a rendszer működtetéséhez szükséges dokumentációk, leírások, szabályzatok minden érintett munkavállaló részére folyamatosan elérhetők legyenek.

Incidensek kezelésének oktatása

A Szolgáltató rendszeres felkészítő oktatást tart a váratlan események, incidensek megfelelő kezelésére. A rendszereket üzemeltető munkatársak között mindenkor kialakításra kerül az értesítési lánc, mely pontos követése minden munkatárs esetében kötelező.

9.5. Felhasználók kötelmei az informatikai biztonság érvényesítésében

Az információ érték, ezért szükséges a biztonságos adatkezelésre vonatkozó normák megfogalmazása, betartása.

A Szolgáltató tevékenységében adat- és titokvédelmi kötelezettség terhel minden dolgozót, így az informatikai eszközöknél és eljárásoknál az Informatikai Biztonsági Szabályzat (IBSZ) és mellékleteinek megfelelően kell eljárni.

Az egyes informatikai rendszerekre külön is vonatkozhatnak rendszerspecifikus biztonsági normatívák, amelyeket a felhasználóknak kötelességük időben megismerni és érvényesíteni.

Az informatikai Biztonsági Szabályzat megsértése jogi felelősséget vonhat maga után.

10. Informatikai Biztonsági Irányítási Rendszer

A Szolgáltató a 470/2017. Kormányrendeletben megfogalmazottaknak megfelelően rendelkezik a hatályos jogszabályokat kielégítő fizikai-környezeti védelemmel, számítógépes programokkal/rendszerekkel, nyilvántartásokkal, valamint az ezek ellenőrzésére szolgáló, a kockázatokkal adekvát és az elvárható gondos és körültekintő vezetéshez és megbízható működéshez szükséges kontrollrendszerrel. A kialakított kontrollrendszer biztosítja a tevékenység folyamatos és biztonságos végzéséhez szükséges feltételeket.

A Szolgáltató külön informatikai biztonsági szabályzattal rendelkezik, amit a Szolgáltató saját hatáskörében és bizonyos időközönként felülvizsgál. A Szolgáltató mindenkor gondoskodik arról, hogy az Informatikai Biztonsági Irányítási Rendszerre vonatkozó dokumentumok és utasítások a megfelelő személyek számára elérhetőek legyenek.

10.1. Informatikai biztonsági szolgáltatás

Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével kell meghatározni az informatikai biztonsági és ellenőrzési kapcsolatokat.
A Szolgáltató az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert alakít ki és üzemeltet. A rendszer hálózatfelügyeleti, behatolásvédelmi, naplóállomány kezelési funkciókat lát el.
A Szolgáltató folyamatosan többrétegű biztonsági kontrollt is használ annak érdekében, hogy a biztosítsa a teljes körű informatikai védelmet.
A Szolgáltató az általános biztonsági intézkedések mellett rendszeresen külső/független sérülékenység-vizsgálatokkal és egyéb auditokkal garantálja a rendszer biztonságos üzemeltetését.

10.2. Kockázatértékelés és -kezelés

A Szolgáltató az informatikai kockázatok felmérését, értékelését és a kockázatarányos védelmi intézkedéseket az informatikai rendszerek tervezése, beszerzése, üzemeltetése során minimum évente egyszer, de minden nagyobb változtatás esetén biztosítja. Az informatikai ellenőrzés minden esetben a kockázatfelmérés eredménye alapján kerül meghatározásra.
A Szolgáltató olyan kockázatelemzési és kockázatkezelési folyamatot alkalmaz, mely képes azonosítani az újonnan felfedezett biztonsági réseket, illetve az újabb biztonsági kockázatok felderítéséhez külső forrásokat is igénybe vesz.

10.3. Dokumentációs követelmények

A Szolgáltató:

- Nyilvántartja, és rendszeresen frissíti vagy a szakterülettel frissítteti dokumentumait.
- Gondoskodik arról, hogy az informatikai rendszerének működtetésére vonatkozó szabályzatok, eljárások, utasítások illeszkedjenek a cég dokumentációs struktúrájába.
- Az informatikai biztonsági vezető útján ellenőrzi minden olyan dokumentáció biztosítását, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működéséhez szükséges.
- Dokumentált változáskövetési és változáskezelési rendszert tart fenn. A változáskövetési és változáskezelési rendszer részletes folyamatait, szabályozását az IT Változáskezelési Folyamat nevű dokumentum tartalmazza.
- Évente minimum egy alkalommal ellenőrzi a katasztrófaelhárítási és -helyreállítási dokumentációt.
- Gondoskodik arról, hogy a tesztelést megkövetelő folyamatoknál a tesztelés dokumentálásra kerüljön.
- Dokumentációs követelmények között előírja a beszállítói részére az átadandó - a megrendelésére készített informatikai rendszer(ek) felépítését tartalmazó, működtetéséhez és ellenőrzéséhez szükséges rendszerleírásokat és modelleket, az adatok szintaktikai szabályait, az adatok tárolási szerkezetét tartalmazó - naprakész dokumentációt.
- Gondoskodik az alkalmazott szoftvereszközök jogtisztaságát bizonyító szerződések, illetve az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának meglétéről.

10.4. Az informatikai biztonság ellenőrzése

A Szolgáltató az informatikai biztonság ellenőrzése céljából legalább évente átfogó belső ellenőrzést hajt végre. A belső ellenőrzés mellett külső vizsgálatokat is végeztet annak érdekében, hogy a bizalmi szolgáltatással kapcsolatosan működő rendszerek mindenkor megfeleljenek a jogszabályi és szakmai követelményeknek.
Bármilyen jellegű hiányosság vagy hiba esetén a Szolgáltató haladéktalanul intézkedéseket tesz a hiányosság/hiba elhárítására, melyeket ellenőriz és dokumentál.

11. Informatikai biztonsági irányelvek, követelmények

A Szolgáltató kiemelt figyelemmel alkotta meg az informatikai biztonsági irányelveket és követelményeket annak érdekében, hogy a bizalmi szolgáltatás a lehető legmagasabb szintű biztonság mellett üzemelhessen.

11.1. A biztonsági rendszer alapvető elemei

A Szolgáltató az informatikai rendszer legfontosabb elemeit (eszközök, folyamatok, személyek) azonosítja.
A Szolgáltató az Informatikai biztonsági vezető által biztosítja az informatikai biztonsági rendszer védelmét, kritikus elemei védelmének zártságát és a biztonsági szempontból teljes körű ellenőrzések lefolytatását, eljárások kialakítását. Az Informatikai biztonsági vezetőnek kezdeményeznie kell a rendszerek saját belső védelmi funkcióinak beállítását és üzemeltetését, valamint a védelmi célú rendszerek telepítését és üzemeltetését.
A Szolgáltató „Hozzáférés kezelés szabályzat” alkalmazása útján biztosítja az informatikai rendszereinek felhasználói adminisztrációját.
A Szolgáltató az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit, valamint a nem rendszeres eseményeket naplózza. A naplózást az üzemeltetési személyzet rendszeresen és érdemben kiértékeli.
A Szolgáltató kiemelt figyelmet fordít a távadatátvitel bizalmasságának, sértetlenségének és hitelességének biztosítására, az adathordozók szabályozott és biztonságos kezelésére, a rendszer vírus- és behatolás-védelmének a biztonsági kockázattal arányos biztosítására.
A Szolgáltató a szolgáltatások folytonosságát biztosító tartalékberendezéseket vagy a szolgáltatások folytonosságát biztosító redundáns rendszereket biztosítja vagy szerződésekkel gondoskodik a megfelelő tartalékok biztosításáról.
A Szolgáltató biztosítja az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől. A fejlesztés- és változásmenedzsment szabályozott körülmények között, dokumentált rendben történik.
A Szolgáltató a szolgáltatások biztonságos ellátásához biztosítja, hogy az informatikai rendszer szoftverelemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend) bírjon, amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket tűzbiztos módon tárolja, valamint gondoskodik a mentések felvételének, visszatöltésének szabályozott, ellenőrzött módjáról. A mentések, archívumok őrzési ideje a jogszabályban előírt időtartamnál rövidebb nem lehet.
A Szolgáltató az informatikai rendszer kivonása esetén az Informatikai biztonsági vezető szakmai felügyelete mellett biztosítja a rendszerrel kezelt adatok biztonságos archiválását. A rendszerkivonás során gondoskodik arról, hogy a rendszerrel kezelt adatok a későbbiekben elkülönített környezetben, ellenőrzési vagy adat-felhasználási célból visszaállíthatóak legyenek.

11.2. Együttműködés külső szervezetekkel

A Szolgáltató mindenkor gondoskodik arról, hogy a számítógépes rendszerek használatához a szállítók és/vagy előállítók által előírt környezeti feltételek kialakításra kerüljenek.

11.3. Hozzáférés- és jogosultságkezelés

A felhasználók csak a munkakörükhöz szükséges rendszerekhez — előzetes igényjogosultság megítélése alapján — kaphatnak hozzáférési jogokat. A hozzáférés csak a szükséges mértékben és időtartamra kerül

engedélyezésre olyan személyek számára, akiknek a feladataik ellátása és/vagy jogaik gyakorlása érdekében az indokolt (ún. „need to know"-elv).
A munkakör ellátásához szükséges IT alkalmazások körét és azokon belüli szerepkör szükségletet elsődlegesen a közvetlen vezető és az Informatikai biztonsági vezető dönti el.

Egy hálózati szolgáltatáshoz hozzáférést a Szolgáltató által alkalmazott vagy vele érvényes szerződéssel rendelkező olyan Partner (Partner azonosító) kaphat:

- akinek munkavégzéséhez az adott szolgáltatás használata szükséges;
- aki rendelkezik az adott szolgáltatás biztonságos használatához szükséges szakmai, üzleti és információbiztonsági ismeretekkel;
- aki biztonsági vagy egyéb okból (pl. összeférhetetlenség) nem esik korlátozás alá.

A felhasználói és rendszerszintű jogosultságok megkérése, nyilvántartása központilag (a Központi Jogosultságkezelési Rendszeren keresztül) történik.
A hozzáférés- és jogosultságkezelési rendszerben szerepel minden rendszerkomponens. Minden rendszerelemen működik jogosultságkezelés.
A jogosultságkezelő rendszer biztosítja, hogy a jogosultságok munkakörönként és funkciónként elkülöníthetők legyenek.
A jogosultságkezelő rendszer képes arra, hogy a több felhasználó által használt rendszerelemeken korlátozni lehessen a felhasználók jogosultságait aszerint, hogy az egyes személyek kizárólag a feladatukhoz szükséges részekhez férjenek hozzá. A jogosultságkezelő rendszerben a "minden tiltva" alapbeállítás kell, hogy szerepeljen.
A hozzáférési jogosultságok az egyének munkakörének és funkciójának figyelembevételével kerülnek megadásra.
A rendszerelemekhez, valamint a kártyaadatokhoz kizárólag azok a személyek kaphatnak hozzáférést, akiknek a munkájához tartozó feladatköre azt valóban megköveteli.
A hozzáférési jogosultságokat dokumentált, írásos vagy elektronikus formában lehet megkérni. A hozzáférési jogosultság kérésénél az érintett rendszert meg kell nevezni, valamint a jogosultságkérést meg kell indokolni.
A hozzáférési jogosultságokat kizárólag az arra kijelölt személy engedélyezheti. A hozzáférési jogosultságok beállítását kizárólag az engedélyezést követően lehet megtenni. A jogosultságok megadásához mindenkor a vonatkozó szabályzatnak megfelelő két engedély, aláírás szükséges. A hozzáféréskezelési rendszer alapbeállítása a „minden tiltása”.
A hozzáférések kérésének és engedélyezésének folyamatát a „Hozzáférés kezelés szabályzat” dokumentum tartalmazza.
A hozzáférések ellenőrzésének folyamatát a „Hozzáférés kezelés szabályzat” dokumentum tartalmazza.

11.4. Logikai védelem

A Szolgáltató az egyes IT rendszereken belül szerepkör, feladat, felelősség és hatókör szerint elhatárolt csoportokat hoz létre, minimálisan az alábbi kategóriákban:

- Rendszergazda(/ák);
- Felhasználó(k);

Továbbá meg kell határozni az egyes kategórián belüli műveleteket:

- adatok, adatcsoportok létrehozása, felvitele;
- adattartalom módosítása;
- adatok lekérdezése;
- adattörlés;
- adatmásolás.

11.5. Fizikai biztonság

A Szolgáltató a bizalmi szolgáltatáshoz használt rendszerek tekintetében két adatközpontot üzemeltet az alábbi címeken, ami a Rackforest Kft. működtetése alatt áll:

1. XIII. kerület 1132 Budapest, Victor Hugo u. 18-22., 3. em.
2. VIII. kerület 1087 Budapest, Asztalos Sándor u. 13.

Mindkét adatközpont megfelel a szükséges fizikai, biztonsági és védelmi követelménynek. A fizikai hozzáférés tekintetében a Szolgáltató meghatározta a szükséges korlátozásokat.

11.6. Hálózatbiztonság

A Szolgáltató rendszerét úgy alakította ki, hogy a hálózat felépítése és működése alkalmas legyen a hálózat biztonságos üzemeltetésére. A Szolgáltató többszörös védelmi vonalakat/biztonsági kontrollokat alkalmaz a legmagasabb szintű biztonság érdekében.
A Szolgáltató magas szintű védelemhez alkalmas tűzfalas védelmet alkalmaz a hálózatok biztonsága érdekében, illetve mindenkor biztosítja, hogy az adatforgalom minden résztvevő és a belső rendszeregységek között is biztonságos csatornán történjen.
A hálózati biztonság esetében a Szolgáltató minimum évente átfogó vizsgálatot tart, illetve egyedi rendszerességgel külső (független) auditot végeztet.

11.7. Üzemeltetési tevékenységek

A Szolgáltató mindenkori informatikai biztonsági felelőse garantálja, hogy a számítógépes rendszerek használatához a szállítók és/vagy előállítók által előírt környezeti feltételek biztosítottak és a kialakított kontrollrendszer naprakészen tartva működik. A naprakészen-tartás keretében a Szolgáltató informatikai biztonsági felelőse gondoskodik az egyes rendszerelemek szükséges frissítéseinek elvégzéséről, az előírt biztonsági beállításokról és a rendszerek folyamatos monitorozásáról.

11.8. Naplózás

A Szolgáltató által üzemeltetett informatikai rendszer működtetése során a rendszert használók tevékenysége és a legfontosabb események naplózásra kerülnek és az eseménynapló-állományok képezik a biztonsági vizsgálatok egyik bizonyítékát.
A naplófájlokban rögzítésre kerülnek az egyes rendszerelemek legfontosabb eseményeinek adatai. A Szolgáltató a naplófájlokat 10 évig megőrzi, ezen idő alatt a Szolgáltató folyamatosan gondoskodik az állományok biztonságos tárolásáról.

11.9. Kártékony programok elleni védelem

A Szolgáltató folyamatosan gondoskodik a kártékony programok elleni védelemről. Ennek három alappillére van:

- Teljes körű technikai vírusvédelem, amely alkalmas többek között a vírusok, férgek, trójaiak, adware, kémszoftverek, rootkit-ek elleni hatékony védekezésre.
- Folyamatos belső képzések, mely során a Szolgáltató felkészíti a rendszereket használó munkatársakat az adathalászat és egyéb hasonló veszélyek elleni hatékony védekezésre.
- Rendszeres biztonsági mentés.

11.10. Az informatikai rendszer szoftverelemeivel szemben támasztott követelmények

A Szolgáltató informatikai rendszerében alkalmazott szoftverek együttesen alkalmasak az alábbiak biztosítására:

- A működéshez szükséges és jogszabályban előírt adatok nyilvántartása.
- A szerződésekben vállalt szolgáltatások nyújtása.
- A tárolt adatok ellenőrzése.
- A biztonsági kockázattal arányos logikai védelem és a sérthetetlenség védelme.

A Szolgáltató informatikai rendszereiben csak jogtiszta, az IT üzemeltetési igazgató által engedélyezett szoftverek használhatók.

11.11. Mentés, archiválás

A Szolgáltató az elektronikus aláírás elhelyezését követően az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít. A Szolgáltató a mentett adatállományokat védi a jogosulatlan

módosítástól és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. A Szolgáltató biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek. A Szolgáltató nem bocsát ki tanúsítványt, ezért a megőrzésre vonatkozó 10 éves idő kizárólag a naplófájlokra vonatkozik.

A Szolgáltató az eszközeire vonatkozó tervezési és fejlesztési szabályzatok, szerződések, valamint a kialakított mentési és helyreállítási eljárások, számítógépes programok és tárolt adatok vonatkozásában biztosítja a jogszabályban, a szolgáltatási szabályzatban és a belső eljárási rendben meghatározott határidőn belül a szolgáltatások helyreállíthatóságát.

A Szolgáltató a rendszer adatvédelmi és információ-archiválási funkcióinak működőképességét rendszeresen ellenőrzi.

11.12. Üzletmenet-folytonosság és katasztrófaelhárítás

A Szolgáltató olyan üzletmenet-folytonossági tervvel (BCP) rendelkezik, mely kellően alacsony vállalt kockázat mellett képes biztosítani a minimálisan elvárt szolgáltatási szinthez szükséges feltételeket és erőforrásokat.

A Szolgáltató rendelkezik katasztrófatervvel (DRP), melyet a katasztrófahelyzetre történő felkészülés során a katasztrófa bekövetkeztekor és a katasztrófa után, a megelőző állapotra történő visszaállás során alkalmaz.

11.13. Bizalmi szolgáltatások tervezése, fejlesztése és tesztelése

A Szolgáltató a bizalmi szolgáltatások tervezése, fejlesztése és tesztelése során a legmagasabb szintű gondossággal jár el. Folyamatosan gondoskodik az éles és a tesztrendszerek megfelelő működtetéséről és a rendszerekben történő változtatások mindenkori automata és manuális teszteléséről.
A kontrollfolyamatok kialakítása során biztosítja, hogy az éles rendszerben az egyes fejlesztésekhez történő változtatások kizárólag teljes körű tesztelést követően kerülhetnek végrehajtásra.

11.14. Változások kezelése

A Szolgáltató a változások kezelésére alapvető irányelvekkel rendelkezik, melyek biztosítják a zavartalan működést.

11.15. Rendkívüli események kezelése

A Szolgáltató a felmerülő incidensek kezelésre belső eljárásrenddel rendelkezik. A belső szabályoknak megfelelően minden incidens esetében a vonatkozó eljárásrend rendelkezései alapján kell eljárni.

12. Megszűnés

A Felek között határozatlan idejű bizalmi szolgáltatásra vonatkozó szerződés jön létre, mely megszűnik:

- a Szolgáltató jogutód nélküli megszűnése esetén,
- az Ügyfél jogutód nélküli megszűnése esetén,
- a Felek közös megegyezésével,
- rendkívüli felmondással,
- rendes felmondással.

Amennyiben a Szolgáltató a jelen Bizalmi Szolgáltatási Szabályzat tárgyát képező szolgáltatási tevékenységével fel kíván hagyni, akkor legkésőbb a tevékenység megszüntetésekor értesíti az Ügyfeleket és a Bizalmi Felügyeletet. Amennyiben a Szolgáltató ellen megszüntetési eljárás indult, akkor ennek tényéről a Szolgáltató haladéktalanul tájékoztatja a Bizalmi Felügyeletet.
A Szolgáltató a bizalmi szolgáltatási tevékenység megszüntetésekor teljes körű biztonsági mentést készít a szolgáltatási tevékenységgel összefüggő adatokról. A Szolgáltató biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.
A szolgáltatás megszüntetésével kapcsolatban a Szolgáltató megjelöli azt a bizalmi szolgáltatót, amely biztosítja a jelen Bizalmi Szolgáltatási Szabályzat hatálya alá tartozó, megszüntetni kívánt bizalmi szolgáltatással összefüggő, a

nyilvánosság számára elérhető nyilvántartásaihoz való hozzáférést és a Szolgáltató gondoskodik a hozzáférési kötelezettség alá eső nyilvántartási adatoknak az átvevő bizalmi szolgáltatónak történő átadásáról.