ADATVÉDELMI

szabályzat

1. Az Adatvédelmi Szabályzat (továbbiakban: Szabályzat) célja

1.1. Az **EXIM CAPITAL INVESTMENT Zártkörűen Működő Részvénytársaság** (továbbiakban - **Társaság)** belső ellenőrzési rendszerének – **belső védelmi vonalainak** - elemei az adatok védelmének biztosítása. A szabályzat célja az adatok és egyes erőforrások biztonság-érzékenysége megállapításának szabályozása annak érdekében, hogy kezelésük, illetve alkalmazásuk során a biztonság érzékenységükkel arányos erősségű védelmet határozzanak meg számukra.

2. A Szabályzat tárgya

2.1. A jelen szabályzat tárgya az adatok, információk biztonságos kezelésének szabályozása. Egyes adatok, információk biztonságos kezelésének rendjét az Informatikai Biztonsági Szabályzat, Iratkezelési Szabályzat valamint az Leltározási és Selejtezési Szabályzat is szabályozza. Az ott szabályozott kérdésekben az Informatikai Biztonsági Szabályzat, Iratkezelési Szabályzat valamint az Leltározási és Selejtezési Szabályzat rendelkezéseit kell használni.

2.2. Jelen szabályzat tárgya továbbá az adatok, és egyes erőforrások biztonság érzékenységének biztonsági fokozatonkénti megállapítása.

3. **A Szabályzat hatálya**

3.1. A Szabályzat tárgyi hatálya kiterjed a Társaság valamennyi, alanyi hatály alá tartozó személy (munkavállaló, alvállalkozó, stb) által folytatott valamennyi adatra, számítógépes és manuális adatkezelésre, illetve adatfeldolgozásra.

3.2. A Szabályzat alanyi hatálya kiterjed a Társaság

a.) munkaviszony alapján foglalkoztatott munkatársaira,
b.) szerződéses jogviszony alapján munkafeladatot végrehajtókra,
c.) vezető tisztségviselőkre,
d.) titoktartási nyilatkozat aláírását követően munkafeladatot végrehajtókra.

3.3. A Szabályzat időbeli hatálya aláírásától módosításáig, visszavonásáig terjed

4. **Jelen Szabályzat során alkalmazott fogalmak meghatározása:**

Az adat tények, elképzelések, utasítások formalizált ábrázolása ismertetés, (tovább) feldolgozás, illetve távközlés céljára. (a személyes adatok, az adatok egy részét képezik).
Az információ fogalma az adat fogalmával megegyezik.
Az adatkezelés az alkalmazott eljárástól függetlenül az adatok felvétele, tárolása, hasznosítása, továbbá adatkezelésnek minősül az adatok megváltoztatása, és a további felhasználás megakadályozása is.
Eszköz a hardver, rendszer szoftver, alkalmazói szoftver, vagy más az adatok manuális vagy gépi kezelését, és az erőforrások kiszolgálását szolgáló berendezés (pl. papír, és elektronikus adathordozók, sokszorosító gép, légkondicionáló berendezés, felvonó).
Az adatvédelem a személyes adatok jogszabályoknak, és a Társaság belső szabályainak megfelelő védelmének szabályozása.
Az adatbiztonság az adatok bizalmasságának, sértetlenségének, és/vagy rendelkezésre állásának minimális fenyegetettsége.
Az osztályozás az adatok, és egyes erőforrások biztonság érzékenységének megfelelő biztonsági osztályokba sorolása. (osztályba sorolás).
Adatfelelős az SZMSZ-ben megjelölt adatvédelmi felelős.

Szigorúan titokban tartandó adat: minden olyan az olyan adat, tény, információ, amely banktitkot, üzleti titkot, szolgálati titkot, vagy személyes adatot tartalmaz, és amelyeknek jogosulatlan harmadik személy általi illetéktelen megszerzése a Társasággal szembeni hatósági eljárás alapját képezheti.
Kiemelten védendő titok: Kiemelten védendő titoknak minősül az olyan adat, tény, információ, amelynek illetéktelen személy tudomására jutása a Társaság, **prudens tevékenységét** megakadályozná, vagy súlyosan veszélyeztetné.
Védendő jelentős titok: Védendő jelentős titoknak minősül az olyan adat, tény, információ, amelynek illetéktelen személy tudomására jutása a Társaság jogos érdekeit **súlyosan** sértené, vagy súlyosan veszélyeztetné, de a prudens működést nem korlátozza vagy veszélyezteti.
Védendő titok: Védendő titoknak minősül az olyan adat, tény, információ, amelynek illetéktelen személy tudomására jutása a Társaság érdekeit enyhébb fokban sértené, vagy veszélyeztetné.

5. Védendő adat és titok a Társaságnál

5.1. Banktitok

Banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

5.2. Üzleti titok

Az üzleti titok fogalma alatt a Polgári Törvénykönyvről szóló 2013. évi V. törvényben meghatározott fogalmat kell érteni.

5.3. Szolgálati titok

Minden olyan, a Társaság tevékenységéhez kapcsolódó tény, információ, megoldás vagy adat, amelynek a titokban maradásához a Társaságnak méltányolható érdeke fűződik, és amely információ, adat nem szerepel közhiteles nyilvántartásban, illetve amely nem kerül közzétételre.

5.4. 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;

6. A biztonsági osztályozás

6.1. Adatok osztályozása:

„A osztály" (szigorúan titkos)
Ide tartozik valamennyi, a jogszabályi előírások alapján szigorúan titokban tartandó adat, továbbá valamennyi olyan adat, amely a Társaság szolgáltatásainak biztonsága, vagy a Társaság üzleti érdekei alapján az arra jogosultak **kiemelten védendő titoknak** sorolnak be.

„B osztály" (titkos)
Ide tartozik valamennyi, a jogszabályi előírások alapján titokban tartandó adat, továbbá valamennyi olyan adat, amelyet a Társaság üzleti érdekei alapján az arra jogosultak **védendő jelentős titoknak** sorolnak be.

„C osztály" (bizalmas)
Ide tartozik valamennyi olyan adat, amelyet a Társaság üzleti érdekei alapján az arra jogosultak **védendő titoknak sorolnak be.**

„D osztály" (nem osztályozott adatok)
Ide tartoznak a **titkot nem képező**, nem biztonság érzékeny adatok.

6.2. Helyiségek osztályozása
„A osztályú, zárt helyiség"
Ide tartozik minden a Társaság üzleti érdekei szerint, a rendeltetése alapján **kiemelten védendő titkot** tartalmazó helyiség.

„B osztályú, kiemelten ellenőrzött helyiség"
Ide tartozik minden a Társaság üzleti érdekei szerint, a rendeltetése alapján **védendő jelentős titkot** tartalmazó helyiség.

„C osztályú, ellenőrzött helyiség"
Ide tartozik minden a Társaság üzleti érdekei szerint, a rendeltetése alapján **védendő titkot tartalmazó** helyiség.

„D osztályú, nem osztályozott helyiség"
Ide tartoznak a rendeltetésük alapján **védendő titkot nem tartalmazó**, nem biztonság érzékeny helyiségek.

6.3. Eszközök osztályozása
„A osztályú, szigorúan titkos eszköz"
Ide tartozik minden a Társaság üzleti érdekei vagy a rendeltetése alapján **kiemelten védendő titkot** képező eszköz.

„B osztályú, titkos eszköz"
Ide tartozik minden a Társaság üzleti érdekei szerint, a rendeltetése alapján **védendő jelentős titkot** tartalmazó eszköz.

„C osztályú, bizalmas eszköz"
Ide tartozik minden a Társaság üzleti érdekei szerint, a rendeltetése alapján védendő **titkot** képező eszköz.

„D osztályú, nem osztályozott eszköz"
Ide tartoznak a rendeltetésük alapján **titkot nem tartalmazó**, nem biztonság érzékeny eszközök.

6.4. Az egyes osztályok szerinti besorolásokat az 1. számú mellékletként csatolt Titokköri Jegyzék tartalmazza.

7. Biztonsági osztályozás folyamata

7.1. Adat, információ, osztályozása az érintett területet a Társaság Szervezeti és Működési Szabályzata (SZMSZ) szerinti adatvédelmi felelős kötelezettsége.

7.2. Adat, információ helyiség biztonsági osztályozását a keletkezésekor, illetőleg a Társaság általi birtokbavételkor kell elvégezni a Titokköri Jegyzék és a Társaság Informatikai Biztonsági Szabályzata szerint és alapján.

7.3. Adat, információ, helyiség biztonsági besorolásának módosítására a besorolást végző adatvédelmi felelős, illetőleg az ügyvezető jogosult.

7.4. Titokköri jegyzék módosítására az adatvédelmi felelős – a besorolásra jogosult adatfelelős, illetőleg az ügyvezető kezdeményezésére – jogosult.

8. A biztonság érzékeny erőforrások védelme

8.1. A védelem tárgya

8.1.1. A védelem tárgya az erőforrások **bizalmassága,** azaz a felfedés elleni védelmük, a **sértetlensége**, azaz a módosítás elleni védelmük, és a **rendelkezésre állásuk**, azaz a megsemmisülésük (eltulajdonításuk) elleni védelmük. A kontrol (védelmi) intézkedéseket a biztonsági szabályozások tartalmazzák.

8.2. A védelem erőssége

Szükséges, hogy a védelem erőssége, – amelyet a biztonsági osztályba sorolás szerint a biztonsági szabályozásokban rendelnek hozzájuk, – az A osztályban a legerősebb legyen, és attól lejjebb fokozatosan gyengüljön.

Védelmi osztályok	**A védendő**			**A hozzáférés**	
	Bizalmasság	Sértetlenség	Rendelke-zésre állás	Belső*	Külső**
A. osztály	Igen kritikus	Kritikus	Folytonos	Erősen korlátozott	Nem engedélyezett
B. osztály	Kritikus	Nagyon fontos	Folytonos	Korlátozott	Erősen korlátozott
C. osztály	Nem kritikus	Fontos	Növelt redundancia	Nem korlátozott	Korlátozott
D. osztály	Nem kritikus	Nem kritikus	Redundancia	Nem korlátozott	Nem korlátozott

* bizalmas hálózaton belül ** nem bizalmas hálózat felé

9. Az adatok, és egyéb erőforrások kezelésének rendje

9.1. A folyamatok osztályozása

Az üzleti folyamatok, informatikai alkalmazások, és támogató folyamatok biztonsági osztályba sorolását az érintett adatfelelősök határozzák meg, a 6. pont alapján.

9.2. A biztonsági osztályozás megőrzése

Az adatoknak a biztonsági osztályozásukat meg kell őrizni az adathordozó (papír vagy elektronikus) változásától függetlenül.

9.3. A tárolás, üzemeltetés, karbantartás rendje:

Az osztályozott helyiségek nem nyílhatnak az osztályozásukkal csak azonos osztályozású vagy egy osztállyal alacsonyabb/magasabb osztályozású helyiségből.

9.4. Az eszközök osztályozása a tárolt adatok, alkalmazások szerint:

Az eszközök, amennyiben osztályozott adatot, szoftvert, alkalmazást tárolnak (pl. notebook) maguk is osztályozottak, és az osztályozással megegyező módon kell kezelni őket.

9.5. A selejtezés

Az osztályozott erőforrásokat a Leltározási és Selejtezési Szabályzat szerint kell selejtezni.

10. Az adatvédelmi felelős

10.1. Szervezeti elhelyezkedése:

Az adatvédelmi felelős olyan munkaviszony, vagy tartós megbízási jogviszony alapján foglalkoztatott munkatárs, aki az ügyvezető közvetlen alárendeltségébe tartozik.

10.2. Az adat-, és titokvédelmi felelős feladatai különösen:

- Releváns jogszabályok módosításának követése, a szabályzaton történő átvezetésének kezdeményezése,
- A Szabályzat naprakészen tartása, és az egyes változatokról, módosításokról a munkatársak tájékoztatása.
- A titokköri jegyzékbe felvétel, és törlés az adatfelelősök illetőleg az ügyvezető állásfoglalásai alapján, figyelembe véve a Szabályzatot.
- A Szabályzat előírásai végrehajtásának felügyelete.
- A Szabályzat végrehajtásával kapcsolatban keletkező jegyzőkönyvek archiválása.
- A biztonsági szabályozások készítőivel, karbantartóival konzultáció, a Szabályzat hatályosítása érdekében.
- A Szabályzat hatókörébe tartozó biztonsági események esetén, a Szabályzat alapján az esemény osztályozása.
- A Szabályzat felső vezetőknek történő oktatásának előkészítése, megszervezése. Az oktatásról jelenléti ív, és a hallgatók tudomásul vételi nyilatkozatának felvétele, megőrzése
- Az új belépő munkatársak oktatása
- Évente legalább egy alkalommal felülvizsgálni a Szabályzat rendelkezéseit.

11. Elsődlegesen figyelembe vett jogszabályok, szabványok

Jogszabályok

- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
- 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

Szabványok

- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények Magyar Szabvány
- FIPS PUB 140-2. Security Requirements for Cryptographic modules. May 25. 2001. NIST,

11. A szabályzat hatályba lépésének időpontja:

Az adatvédelmi szabályzat az aláírás napján lép hatályba.

Budapest, 2019. december 6.

……..
Igazgatóság nevében
Igazgatóság elnöke

Mellékletek

1. Titokköri jegyzék és függeléke

1. sz. Melléklet

TITOKKÖRI JEGYZÉK

Hatályos: módosításáig

1. ADATOK

1.1. Szigorúan titkos adatok (amelyek vagy Banktitkot, vagy üzleti titkot képeznek, „A" osztály)

- Arra jogosult által ilyen osztályba sorolt adatok;
- A Társasággal szerződésben álló pénzügyi intézmények, és más szervezetek kezelésre átadott, banktitkot képező adatai;
- A nem pénzügyi intézményektől kezelésre átvett adatok;
- A Társaság szerződéses ügyfeleinek adatai, az ügyfelek listája;
- Üzleti folyamatok kockázati mátrixai;
- Belső ellenőrzés ütemtervei és jelentései;
- Minőségbiztosítás adatai;
- Tervezetek, munkaanyagok;
- Alkalmazott szoftverek dokumentációja;
- Jogi adatok;
- A pénzügyi, számviteli adatok;
- Kontrolling adatok;
- Társaság archivált adatai ;
- banki szoftver és a hozzá kapcsolódó adatbázis;

1.2. Titkos adatok (Személyes adatok, „B" osztály)

- Arra jogosult által ilyennek sorolt adatok;
- Informatikai Biztonsági Szabályzat;
- A naplók adatai (audit trail, audit log, behatolási log a fizikai belépés ellenőrzés adatai, a biztonsági felügyelet naplója);
- A Társaság munkatársai személyi anyagai (munkaszerződések, önéletrajzok, bizonyítványok, stb.);
- A munkatársak humánpolitikai adatai;
- A bérlisták;
- A harmadik felek szerződés alapján a Társaság területén feladatot teljesítő munkatársainak adatai;
- Felügyeleti intézkedések, határozatok;
- Az Igazgatósági, Felügyelő Bizottsági ülések anyagai;
- Szervezeti Működési Szabályzat;
- Telefonjegyzék;
- Fájl szerveren tárolt dokumentumok;

1.3. Bizalmas adatok („C" osztály)

- Arra jogosult által ilyennek sorolt adatok;
- Közgyűlési anyagok;
- Vezetői értekezletek anyagai;
- Cégiratok;

- Az „A” és „B” osztályba nem sorolt informatikai biztonsági szabályozások, valamint az Adatvédelmi Szabályzat;
- Belső ellenőri szabályozások, a mellékleteket kivéve;
- Társaság szolgáltató illetve szállító partnerei szerződései;
- Marketing tervek, programok;
- Levelező rendszer;

1.4. Nem osztályozott adatok („D” osztály)

- Közzétételre készített mérleg-, és cégadatok;
- Reklám, és propagandaanyagok;
- Oktatási anyagok;
- Vállalati stratégia;
- Üzleti, és Informatikai Stratégia;

2. ALKALMAZÁSOK, ÜZLETI FOLYAMATOK

A 6. pontban megadott osztályozásnak megfelelően besorolva

Üzleti folyamatok („A” osztály)

- Az üzleti folyamatokat kiszolgáló informatikai alkalmazások;

Támogató folyamatok („B” osztály)

- Erőforrások üzemeltetése;
- Szabványosítás;
- Értékesítés, marketing;
- Pénzügy;
- Bérszámfejtés;
- Jogi képviselet;
- Minőségbiztosítás;
- Kontrolling;
- Vállalatirányítás;
- Humán erőforrás gazdálkodás;
- Belső ellenőrzés;

3. HELYISÉGEK

Zárt helyiségek („A” osztály)

Kiemelten ellenőrzött helyiségek („B” osztály)

- Belső ellenőr irodája
- Központi hálózati eszközöket tartalmazó helység
- Ellenőrzött helyiségek („C” osztály)
- A Kiemelten ellenőrzött helyiségek osztályban fel nem sorolt irodák, tanács-, és oktató termek

Nem osztályozott helyiségek („D” osztály)

- Ügyfélfogadó (Recepciók előterei)

4. ESZKÖZÖK

Szigorúan titkos eszközök („A” osztály)

- Számítástechnikai eszközök, ha osztályozott anyagot tárolnak, kezelnek
- A naplók

Nem osztályozott eszközök („C” osztály)

- Minden egyéb eszköz