DUNAFERR SE

Adatbiztonsági Szabályzat

1. Bevezetés

Ez a dokumentum ismerteti a Dunaferr Sportegyesület (a továbbiakban: "Egyesület") elnökének intézkedését amelyet az Egyesület számítógépes rendszerének, eszközeinek és minden más adattárolási eszközeinek védelmére dolgoztak ki.

2. Alapelvek

1. Minden informatikai és fizika adattároló rendszert (továbbiakban: adattároló rendszerek) védeni kell az illetéktelen hozzáféréstől.
2. Az adattároló rendszereket csak a vonatkozó Egyesületi irányelvekkel összhangban lehet alkalmazni.
3. Az Egyesület vezetőségi tagja és az összes adattároló rendszer használatára feljogosított valamennyi harmadik fél, ideértve, az alvállalkozókat (együttesen "Felhasználók") kötelesek elolvasni és betartani jelen szabályzatot.
4. Az adattároló renszereken tárolt valamennyi adatot biztonságosan kell kezelni az EU 2016/679 általános rendeletének ("GDPR"), valamint az adatvédelmet szabályozó minden más jogszabálynak megfelelően.
5. Az összes kezelt adatot megfelelő kategóriába kell sorolni (pl.: személyes adatok, különleges adatok és bizalmas információk) a GDPR információs és feldolgozási dokumentumra való hivatkozással. Az így kategorizált összes adatot az osztályozásnak megfelelően kell kezelni.
6. Az adattároló rendszereken tárolt adatok csak azoknak a felhasználóknak áll rendelkezésre, akik jogosultak a hozzáféréshez.
7. Az adattároló rendszereken tárolt összes adatot védeni kell az illetéktelen hozzáféréstől, feldolgozástól és megsemmisüléstől.
8. Az adattároló rendszerek biztonsága és integritása, valamint az ezeken tárolt adatok (beleértve, az adatok biztonságát, sértetlenségét és titkosságát) az egyesületi elnök felelőssége, kivéve, ha az egyesület kifejezetten másként rendelkezik.
9. Az adattároló rendszerek vagy az azokon tárolt összes adatbiztonság sérülését az egyesület elnökének jelenteni kell, majd ezt követően ki kell vizsgálni.
10. A felhasználókak jelenteniük kell az adattároló rendszerekkel kapcsolatos összes biztonsági aggályt vagy észrevételt az elnök felé.

3. Az elnök mint adatvédelmi megbízott feladata:

Mátyás Gábor a Dunaferr Sportegyesület elnöke vagy felhatalmazottja felelős a következőkért:

3.1. biztosítja, hogy az összes adattároló rendszer megfeleljen az egyesület biztonsági követelményeinek;

3.2. biztosítja az egyesületen belüli adatbiztonsági szabályok hatékony végerhajtását és rendszeres felülvizsgálatát;

3.3. biztosítja, hogy minden felhasználó tisztában legyen a jelen irányelvel, minden kapcsolódó jogszabállyal, rendelettel és egyéb vonatkozó szabályok követelményeivel, ideértve többek között a GDPR-t és a számítógépes visszaélésről szóló 1990. évi törvényt;

3.4. segítséget nyújt minden felhasználónak e szabályzat megértésében és betartásában;

3.5. minden felhasználó számára megfelelő támogatást és képzést biztosít az adatbiztonsági kérdésekben és az adattároló rendszerek használatában;

3.6. biztosítja, hogy minden felhasználó hozzáférhessen az adattároló rendszerekhez, figyelembe véve munkájukat, felelősségüket és a különleges biztonsági követelményeket;

3.7. az adatbiztonsági kérdésekkel kapcsolatos valamennyi jelentés kézhezvétele és kezelése, valamint megfelelő válaszintézkedések megtétele;

3.8. proaktív fellépést biztosít, az adatbiztonsági eljárások létrehozása és végrehajtása, valamint a felhasználók tudatosságának növelése érdekében;

3.9. biztosítja, hogy az informatikai rendszereken belül tárolt összes adatról rendszeres biztonsági másolat készül, lehetőség és vagy szükség esetén napi rendszerességgel. Minden mentést titkosítani kell.

4. A felhasználók felelőssége:

4.1. Minden felhasználónak meg kell felelnie a jelen szabályzat összes releváns részének, amikor az adattároló rendszereket használja.

4.2. A felhasználóknak azonnal tájékoztatniuk kell az adatvédelmi felelőst az adattároló rendszerekhez kapcsolódó összes biztonsági aggályról.

4.3. A felhasználóknak azonnal értesíteniük kell azadatvédelmi felelőst bármely más technikai probléma esetén (beleértve, hardver és szoftver hibákat), amelyek az informatikai rendszereken előfordulhatnak.

4.4. A jelen Felhasználási Szabályzat bármely szándékos vagy gondatlan megsértését a egyesület fegyelmi eljárásai szerint kell kezelni.

5. Szoftver biztonsági intézkedések

5.1. Minden informatikai rendszeren (beleértve, az operációs rendszereket, az egyedi szoftveralkalmazásokat) használó szoftvereket naprakészen tartunk, és minden releváns szoftverfrissítést, javítást és egyéb köztes kiadványt az adatbiztonsági felelős kizárólagos döntése alapján alkalmazunk. Ez a rendelkezés nem terjed ki a szoftverek új "főbb kiadásokra" történő frissítésére, csak egy adott fő kiadáson belüli frissítésre.

5.2. Ha bármilyen szoftverhiba azonosításra kerül, a hibát azonnal rögzítjük, vagy a szoftvert az IT-rendszerből visszavonjuk addig, amíg a biztonsági hibát hatékonyan orvosolni nem tudták.

5.3. A felhasználók semmilyen szoftvert nem telepíthetnek, sem fizikai adathordozón sem pedig letöltéssel az adatvédelmi megbízott jóváhagyása nélkül. Minden, a Felhasználóhoz tartozó szoftvert az adatvédelmi megbízottnak jóvá kell hagynia, és csak akkor telepíthető, ha az adott telepítés nem jelent biztonsági kockázatot az IT rendszerek számára, és ha a telepítés nem sért olyan licencszerződést, amely a szoftverre vonatkozik.

5.4. Az IT rendszerekre telepítendő szofvereket csak az informatikai megbízott telepítheti, kivéve, ha az egyes felhasználók számára írásbeli engedélyt nem ad az adatvédelmi megbízott. Az ilyen írásbeli engedélynek világosan jelölnie kell, hogy melyik szoftver telepíthető, és mely számítógépen vagy eszközön telepíthető.

6. Vírusvédelmi biztonsági intézkedések

6.1. A legtöbb IT-rendszert (beleértve az összes számítógépet és szervert) megfelelő vírusvédelem, tűzfal és egyéb megfelelő internetes biztonsági szoftver véd. Minden ilyen szoftver a legújabb naprakész szoftverfrissítésekkel biztosított.

6.2. Minden anti-vírus szoftver által védett IT rendszer rendszeres vizsgálatot igényel.

6.3. A fájlok átvitele során a felhasználók által használt minden fizikai adathordozót (például USB-memóriakártyát vagy lemezeket) vírusvizsgálatnak kell alávetni, mielőtt bármilyen fájl átmenthető. Az ilyen víruskereséseket automatikusan a média csatlakoztatásával / beillesztésével, vagy a felhasználó vagy az adatvédelmi megbízott útján kell végrehajtani.

6.4. Az egyesület harmadik fél felé - akár e-mailben, fizikai adathordozón vagy más eszközzel (pl.: megosztott felhő tárolás) - küldött fájlokon vírus szkennelést kell végezni a küldés előtt vagy a küldő folyamat részeként.

6.5. A Felhasználó bármely vírus észlelést haladéktalanul jelent azadatvédelmi megbízottnak (ez a szabály akkor is érvényes, ha a víruskereső szoftver automatikusan megoldja a problémát). Az adatvédelmi megbízott haladéktalanul megtesz minden szükséges intézkedést a probléma orvoslására. Korlátozott körülmények között ez magába foglalhatja az érintett számítógép vagy eszköz ideiglenes eltávolítását.

6.6. Ha bármelyik felhasználó szándékosan használ esetleges rosszindulatú szoftvert vagy vírust az informatikai rendszerbe, ez az 1990-es Számítógép-visszaélés-

törvény alapján bűncselekménynek minősül, és az egyesület fegyelmi eljárásának megfelelően kezelhető.

7. Hardver biztonsági intézkedések

7.1. Ahol csak lehetséges, az informatikai rendszerek olyan helyiségben helyezkednek el, amelyek biztonságosan zárhatók. Az egyesület minimalizálja az illetéktelen hozzáférések lehetőségét.

7.2. Minden olyan informatikai rendszert, amelyet a felhasználók nem használnak (beleértve, a szervereket, a hálózati eszközöket és a hálózati infrastruktúrát) - ahol lehetséges és praktikus - biztonságos, klimatizált helyiségekben és / vagy zárt szekrényekben kell elhelyezni ahol csak az adatvédelmi megbízott férhet hozzá.

7.3. Az adatvédelmi megbízott kifejezett engedélye nélkü, a felhasználóknak semmi esetben nem lehet hozzáférése olyan IT-rendszerekhez, amelyeket nem a Felhasználók használatára szántak. Normál körülmények között, amikor az ilyen informatikai rendszerekkel kapcsolatos problémákat a Felhasználó azonosítja, ezt a problémát jelenteni kell az adatvédelmi megbízottnak. A Felhasználó semmilyen körülmények között ne próbálhatja meg orvosolni az ilyen problémát az adatvédelmi megbízott kifejezett engedélye, utasítás és / vagy felügyelete nélkül.

7.4. Minden nem mobil eszköz (beleértve, asztali számítógépeket, munkaállomásokat és monitorokat), ahol lehetséges és praktikus, megfelelő rögzítő mechanizmussal kell biztosítani. Ahol a hardver kialakítása lehetővé teszi, a számítógép dobozt le kell zármi, hogy megakadályozzák a belső alkatrészek meghamisítását vagy lopását.

7.5. Minden mobil eszközt (pl.: laptopok, tábalgépek és okostelefonok) biztonságosan kell szállítani és gondosan kell kezelni. A felhasználóknak minden ésszerű erőfeszítést meg kell tenniük annak elkerülése érdekében, hogy az ilyen mobil eszközöket ne hagyják felügyelet nélkül, kivéve saját otthonukban vagy a vállalat telephelyén. Ha a mobil eszközt járműben kell hagyni, mindeképpen nem látható helyre kell rejteni és lehetőség szerint zárt térben kell tárolni.

8. Hozzáférés

8.1.Az összes adattárolási rendszerhez való hozzáférési jogokat az egyesületen belüli felhasználói jogosultsági szintek és munkaköri feladatok alapján kell meghatározni.

8.2. Minden informatikai rendszert (ide értve a mobil eszközöket, laptopokat, táblagépeket és okostelefonokat) jelszóval, pinkóddal vagy a biztonságos bejelentkezési rendszer más formájával kell védeni. A biometrikus bejelentkezés nem minden formája tekinthető biztonságosnak. Csak az informatikai szakember által jóváhagyott módszereket lehet alkalmazni.

8.3. Minden jelszó, ahol a szoftver, a számítógép vagy az eszköz lehetővé teszi:

a) legalább 15 karakter hosszú legyen;
b) tartalmazzon kis- és nagybetűket, számokat és szimbólumokat;

c) véletlenszerűen legyen generálva egy jelszó szoftver segítségével, például Keepass;
d) különbözzön az előző jelszótól;
e) ne legyen nyilvánvaló vagy könnyen kitalálható (például születésnapok vagy más emlékezetes dátumok, emlékezetes nevek, események vagy helyek stb.); és
f) minden felhasználónak külön felhasználó kódja legyen.

8.4. A jelszót minden felhasználónak titokban kell tartania. A felhasználó semmilyen körülmények között ne ossza meg jelszavát senkivel. Senki nem kérheti el a felhasználó jelszavát, és minden ilyen nemű kérést el kell utasítani. Ha a felhasználónak oka van feltételezni, hogy egy másik személy megszerezte a jelszavát, haladéktalanul módosítania kell a jelszót és jelentenie kell az incidenst az adatvédelmi megbízottnak.

8.5. Ha a felhasználó elfelejti jelszavát, ezt jelentenie kell az adatvédelmi megbízottnak. Az informatikai megbízott megteszi a szükséges lépéseket annak érdekében, hogy visszaállítsa a felhasználó hozzáférését az adattároló rendszerhez ez magában foglalhatja az ideiglenes jelszó kiadását, amely teljes mértékben vagy részben megismerhető a probléma megoldására illetékes informatikai személyzet tagjával.

8.6. A felhasználónak azonnal új jelszót kell létrehoznia az IT-rendszerekhez való hozzáférés visszaállítása után.

8.7. Ha a felhasználó meg tudja jegyezni a jelszót, akkor ne írja azt le sehova. Ha a felhasználó nem tudja memorizálni a jelszót akkor, azt biztonságosan kell tárolni valahol (pl. zárolt fiókban vagy biztonságos jelszó-adatbázisban), és semmilyen körülmények között sem szabad azt mások részére megjeleníteni.

8.8. Minden kijelzővel és felhasználói beviteli eszközzel (pl. egér, billentyűzet, érintőképernyő stb.) Rendelkező IT-rendszert védeni kell, ahol lehetséges, egy jelszóval védett képernyővédővel, amely 10 perc inaktivitás után aktiválódik. Ez az időzóna nem módosítható a felhasználók által és a felhasználók nem tilthatják le a képernyővédőt. A képernyővédő aktiválása nem szakítja vagy zavarja meg a számítógépen végrehajtott egyéb tevékenységeket (pl. Adatfeldolgozás).

8.9. Az egyesület által biztosított összes mobileszköz (pl.: laptopok, táblagépek és okostelefonok) 10 perc inaktivitás után “sleep” módra van állítva, ez után jelszó vagy pikkód bevitelt igényel a feloldáshoz. A felhasználók nem módosíthatják ezt a beállítást.

8.10. A felhasználók nem használhatnak semmilyen olyan szoftvert, amely külső személy számára lehetővé teheti az informatikai rendszerek elérését az adatvédelmi felelős kifejezett hozzájárulása nélkül.

9. Adattárolási biztonság

9.1. Minden adatot, különösen a személyes adatokat biztonságosan kell tárolni jelszavak adat titkosítás és zárt szekrények útján.

9.2. A fizikai adathordozón, elektronikusan elmentett összes személyes adatot biztonságosan kell tárolni zárt dobozban, fiókban, szekrényben vagy más hasonló helyen.

10. Adatvédelem

10.1. Az egyesületáltal összegyűjtött, tárolt és feldolgozott összes személyes adatot (a GDPR-ben meghatározottak szerint) a GDPR elveivel, a GDPR rendelkezéseivel és az egyesület adatvédelmi politikájával összhangban gyűjtjük, tároljuk és dolgozzuk fel.

10.2. Minden olyan felhasználó és adatkezelő aki az egyesület részére és nevében adatokat kezel, mindenkor meg kell felelnie az egyesület adatvédelmi szabályainak. Különös figyelemmel a következőkre:

a) A személyes adatokat tartalmazó e-maileket lehetőség szerint tikosítani kell.

b) A személyes adatok csak biztonságos hálózatokon keresztül továbbíthatók; semmilyen körülmények között nem engedélyezett a nem biztonságos hálózatokon történő átvitel;

c) Vezeték nélküli hálózaton keresztül nem továbbítunk személyes adatokat, ha van ésszerűen megvalósítható vezetékes alternatíva;

d) Minden fizikailag szállítandó személyes adatot - beleértve a cserélhető elektronikus adathordozón is - bele kell helyezni egy "bizalmas" jelzésű tartóba.

e) Ha bizalmas vagy személyes adatokat jelenítenek meg a számítógép képernyőjén, és a kérdéses számítógépet bármely időtartamra felügyelet nélkül kell hagyni, a felhasználónak le kell zárnia a számítógép képernyőt, mielőtt elhagyná azt.

10.3. Az adatvédelemre vonatkozó kérdéseket Laczkó Bernadett cégvezetőnek kell címezni.

11. Internet és e-mail használat

11.1.Minden felhasználó köteles az egyesületkommunikációs, e-mail és internetes szabályzatának rendelkezéseit betartani, amikor az informatikai rendszereket használja.

12. IT incidensek kezelése

12.1. Minden aggályt és esetleges szabálysértést vagy incidenst azonnal jelenteni kell az adatvédelmi megbízottnak.

12.2. Kérdés vagy értesítés kézhezvétele után az adatvédelmi megbízott 2 napon belül értékeli a kérdést, beleértve, de nem kizárólagosan az ezzel járó kockázati szintet, és minden lépést megtesz, hogy válaszoljon a kérdésre.

12.3. A Felhasználó semmilyen körülmények között sem próbálhatja meg megoldani az informatikai incidenseket anélkül, hogy először konzultálna az adatvédelmi

megbízottal. A felhasználók csak az adatvédelmi megbízott utasításával és kifejezett engedélyével oldhatják meg az informatikai incidenseket.

12.4. Minden informatikai incidenst teljes mértékben dokumentálni kell.

13. Az Adatbiztonsági szabályzat ellenőrzése

Az egyesületnél kezelt személyes adatok tárolásásnak biztonságát az egyesület vezetősége és az általa megbízott adatvédelmi megbízott és informatikus évente egyszer ellenőrzi.

Utolsó frissítés időpontja: 2019. január 24.
Következő ellenőrzés időpontja: 2020. január 24.

14. Záró rendelkezések

E szabályzat tartalmát meg kell ismertetni az egyesület valamennyi vezetőségi tagjával, munkavállalójával és alvállalkozójával és a megbízási szerződésekben elő kell írni, hogy betartása és érvényesítése minden vezetőségi tag, munkavállaló és alvállalkozó munkaköri kötelessége.

Az egyesület adatai:

Dunaferr Sportegyesület

Székhely:	2400 Dunaújváros, Eszperantó út 4.
Telefon:	+36 30 848 7359
E-mail:	dunaferrse@digikabel.hu
Weboldal:	dunaferrse.hu
Céginformáció:	07-02-0000038
Adószám:	19820222-2-07

Az Adatbiztonsági Szabályzatot jóváhagyta:

Mátyás Gábor
Dunaferr Sportegyesület Elnöke

DUNAFERR SPORTEGYESÜLET
2400 Dunaújváros, Eszperantó út 4.
19820222-2-07
10300002-10555153-49020017