Információ Biztonsági Szabályzat

Verzió	**TBC**
Jóváhagyó	**TBC**
Hatályba lépés dátuma	**TBC**

Tartalomjegyzék

1. A szabályzat célja 3
2. A szabályzat hatálya 3
3. Jogi háttér 3
4. Szabályozott területek 4
5. Jogosultságkezelés 4
5.1. Jogosultság igénylése 4
5.2. Jogosultság módosítása 5
5.3. Jogosultság törlése, visszavonása 5
5.4. Jogosultságok felülvizsgálata 5
5.5. Kiemelt jogosultságok 5
5.6. Külső hozzáférések 6
5.7. Jelszókezelés 6
5.7.1. Kiemelt felhasználók jelszavai 6
5.8. Felhasználói azonosítók 6
5.9. Fizikai biztonság 7
5.9.1. Beléptetés 7
5.9.2. Szerverek biztonsága 7
6. Felhasználói viselekedés 7
6.1. Mobil eszközök kezelése 7
6.2. E-mail/internethasználat 8
6.3. Biztonságtudatosság 8
6.4. Adathordozók kezelése 8
6.5. Tiszta asztal, tiszta képernyő 9
7. Üzemeltetés biztonsági szempontjai 9
7.1. Rendszerüzemeltetés 9
7.2. **Hálózatbiztonság** 9
7.2.1. Szegmentáció 9
7.2.2. Vezetéknélküli internetkapcsolat (Wifi) 10
7.2.3. Távoli elérés 10
7.2.4. Titkosítás 10
7.2.5. Vírusvédelem 11
7.2.6. Tűzfal 11
7.3. Adatok mentése 11
7.3.1. Mentési folyamatok 11
7.3.2. Visszatöltési eljárások, tesztek 11
7.4. Naplózás 12
7.5. Szoftverek 12
7.6. Kiszervezett tevékenységek 12
8. Fejlesztés 13
8.1. Rendszerfejlesztés ..... **Hiba! A könyvjelző nem létezik.**
8.1.1. Környezetek szétválasztása 13
8.1.2. Fejlesztési folyamat 13
9. Adatkezelés 13
9.1. Adatok megőrzési ideje 13
9.2. Adatok törlése 13
9.2.1. Automatikus 14

9.2.2. Ad-hoc törlés 14
9.3. Adatkinyerés 14
9.4. Adatgazdák feladatai, felelősségei 15
9.5. Információk osztályozása 15
9.5.1. Adatkategóriák 15
10. Információbiztonsági adminisztratív folyamatok 15
10.1. Üzletmenet folytonosság 15
10.1.1. BCP és DRP tervek készítése ..... **Hiba! A könyvjelző nem létezik.**
10.1.2. A tervek tesztelése 15
10.1.3. A tervek felülvizsgálata ..... **Hiba! A könyvjelző nem létezik.**
10.2. Incidensmenedzsment 16
10.2.1. Incidensek észlelése 16
10.2.2. Incidensek kezelése 16
10.2.3. Incidensek dokumentálása 18
10.2.4. Incidensek elemzése, tanulságok levonása 18
11. Kockázatelemzés 18
11.1. Rendszerek osztályozása 18
11.2. Kockázatelemzés elvégzése 19
12. Felülvizsgálat 19

1. A szabályzat célja

Jelen Információbiztonsági Szabályzat (továbbiakban: Szabályzat) célja, hogy egységes keretszabályokat, rendelkezéseket, iránymutatást adjon a Magyar Röplabda Szövetség (továbbiakban "Szövetség" vagy "MRSZ") számára az informatikai biztonság területén.
Továbbá iránymutatást ad a mindenkori vezetés, a munkavállalók és rendszergazdák számára, rögzítve azokat a szabályokat, amelyek betartása szükséges az alapvető információbiztonsági elvárásoknak való megfeleléshez.
A Szabályzat célja továbbá, hogy a Szövetség tevékenysége során kezelt informatikai eszközök, feldolgozott és továbbított adatok bizalmasságát, sértetlenségét biztosítani tudja, valamint a rendelkezésre állást fenyegető veszélyek elhárítására hatékony védelmi intézkedéseket tudjon megfogalmazni.

2. A szabályzat hatálya

A Szabályzat hatálya kiterjed a Szövetség valamennyi szervezeti egységére és munkatársára, valamint minden olyan személyre, aki akár a Szövetség megbízásából, akár bármely más célból használja a Szövetség informatikai infrastruktúráját.
A Szabályzat hatálya kiterjed az MRSZ tulajdonát képező valamennyi informatikai, kommunikációs és adatátviteli eszközre, mely a Szövetség területén, illetve a Szövetséggel munkakapcsolatban álló másik szervezetnél működik, illetve minden olyan nem a Szövetség tulajdonát képező informatikai, kommunikációs és adatátviteli eszközre, mely a Szövetség informatikai rendszerével közvetlen elektronikusan kapcsolatban van. A Szabályzat hatálya az alábbi, a Szövetség által használt rendszerekre terjed ki:

- A Szövetség fájlszervere
- Backoffice rendszer
- KulcsSoft rendszer
- hunvolley.hu
- ropsuli.hu
- EKR rendszer

Fizikai hatálya kiterjed a Szövetség telephelyeire, irodáira, létesítményre is.

3. Jogi háttér

A Szabályzat alapját az Európai Parlament és a Tanács 2016/679 rendelete (továbbiakban: GDPR), az ISO 27001-es szabvány, valamint az iparági jó gyakorlatok képezik.

4. Szabályozott területek

A Szabályzat az információbiztonság alábbi területeit kívánja szabályozni:

- Jogosultságkezelés
- Felhasználói viselkedés
- Üzemeltetés biztonsági szempontjai
- Fejlesztés
- Adatkezelés
- Információbiztonsági adminisztratív folyamatok

5. Jogosultságkezelés

Minden felhasználónak olyan szintű jogosultság engedélyezhető, ami szükséges és éppen elégséges a munkája elvégzéséhez. A jogosultságkezelés során *a legkisebb jogosultság elvé*nek kell megfelelni. Az alábbi fejezetekben részletesen megismerhető a jogosultságkezeléssel kapcsolatos elvárások.

5.1. Jogosultság igénylése

A Szövetség bármely informatikai rendszeréhez jogosultság létrehozása, megadása csak formális igénylés és jóváhagyás után lehetséges. Az igényt e-mailben kell eljuttatni a jóváhagyással együtt a jogosultságot beállító személy számára.
A különböző rendszerek jóváhagyói és felelősei:

Rendszer	Jóváhagyó	Felelős
Fájlszerver	MRSZ főtitkár	Farkas Gábor, MRSZ rendszergazda
Backoffice rendszer	Liszt Katalin, gazdasági vezető	Liszt Katalin továbbítja Oczella László (Számíthat Kft.) részére
KulcsSoft rendszer	Liszt Katalin, gazdasági vezető	Vatai Gabriella
MRSZ tulajdonában lévő honlapok	MRSZ főtitkár	Oláh János, honlap üzemeltető
EKR rendszer	dr. Tamás Henriette, TAO igazgató	Flexinform Kft.

A rendszerek felelőseit és jóváhagyóit a mindenkori Főtitkár nevezi ki e-mailes formában.

5.2. Jogosultság módosítása

Amennyiben a felhasználó munkavégzéséhez adott rendszeren belül további jogosultságra van szüksége, az 5.1. pontban meghatározott jóváhagyó engedélyével állítható be neki a felelős által. Amennyiben a korábbinál kisebb jogkörrel rendelkező jogosultság is elegendő a munkavégzéshez, a módosítási folyamatot abban az esetben is végre kell hajtani.

5.3. Jogosultság törlése, visszavonása

Amennyiben a felhasználó munkavégzéséhez a továbbiakban nem szükséges valamely jogosultság, úgy azt a lehető legrövidebb időn belül törölni kell. A törlést az 5.1. pontban meghatározott felelősök végzik el, a jóváhagyó e-mailes kérése után.
Kilépő munkavállaló esetén a kilépési folyamat részeként a gazdasági vezető jelzi a rendszergazda és az egyéb IT oldali felelősök felé a kilépést (lásd:5.1-es táblázat). A felhasználó minden jogosultságát egy munkanapon belül meg kell szüntetni.

5.4. Jogosultságok felülvizsgálata

A rendszerek 5.1. pontban meghatározott felelősei évente riportot késztenek a jogosultsággal rendelkező felhasználókról és azt az 5.1. pontban meghatározott jóváhagyók számára megküldik felülvizsgálatra. Amennyiben valamelyik felhasználónak nincs szüksége a meglévő jogosultságok valamelyikére, illetve más típusú jogosultságra van szüksége a munkavégzéshez, úgy az 5.2. és 5.3. pontban leírt folyamatokat kell végrehajtani.
Amennyiben valamely munkavállalónak megváltozik a beosztása és/vagy a munkaköre, az előbbi módon ellenőrizni kell milyen jogosultságokkal rendelkezik, és, hogy azok továbbra is szükségesek-e számára.

5.5. Kiemelt jogosultságok

A rendszerekben használatos kiemelt, magas szintű hozzáféréssel rendelkező felhasználókat korlátozni szükséges, kiemelten az adott rendszerek adminisztrátori és beépített rendszerfelhasználói esetében. Ez megvalósulhat rendszertől függően:

- részletes naplózással
- tevékenység megfigyelésével
- felhasználói jogosultság ideiglenes kiadásával
- átlagosnál erősebb biztonsági szintű, komplex jelszavak megkövetelése:
    - a jelszónak kötelezően tartalmaznia kell legalább egy kisbetűt, nagybetűt, számot és speciális karaktert is
    - a jelszónak legalább 12 karakter hosszúnak kell lennie

5.6. Külső hozzáférések

Harmadik félnek hozzáférés az 5.1. pontban meghatározott jóváhagyó írásos jóváhagyásával adható. A külső felek számára biztosított hozzáféréseket évente felül kell vizsgálni az 5.4.-es pont szerint.
A külső felek egyedi, nevesített azonosítóval férhetnek hozzá a Szövetség rendszereihez.

5.7. Jelszókezelés

A Szövetség számítógépes hálózatába, illetve az alkalmazások rendszerébe bejelentkezési névvel rendelkező felhasználó köteles a bejelentkező nevéhez tartozó jelszó megőrzésére. A saját bejelentkező névhez tartozó jelszót elárulni, mások által is elérhető módon feljegyezni nem szabad. Új hozzáférés esetén az első bejelentkezést követően a kezdeti jelszó megváltoztatása kötelező. A kezdeti jelszót a felhasználókhoz másodlagos csatornán keresztül kell eljuttatni.

A jelszavak legalább az alábbi követelményeknek kell megfelelniük:

- legalább 8 karakter hosszú,
- tartalmaz nagybetűt, kisbetűt és számot is,
- 5 sikertelen próbálkozás után a felhasználó automatikusan zárolódik.
- 120 napos lejárati idővel rendelkezik

A jelszavak biztonságát növelni lehet speciális karakterek használatával, illetve a szótári szavak, a felhasználóhoz köthető adatok (pl. háziállat neve, születési dátum) mellőzésével. A meghatározott jelszókövetelmények minden felhasználóra érvényesek.

5.7.1. Kiemelt felhasználók jelszavai

A kiemelt jogosultsággal rendelkező felhasználók esetében az alábbi komplexitási követelményeket kell érvényesíteni:

- a jelszónak kötelezően tartalmaznia kell legalább egy kisbetűt, nagybetűt, számot és speciális karaktert
- a jelszónak legalább 12 karakter hosszúnak kell lennie
- a felhasználó 3 sikertelen próbálkozás után automatikusan zárolódik
- 90 napos lejárati idővel rendelkezik

5.8. Felhasználói azonosítók

Minden felhasználónak egyedi, nevesített felhasználónévvel és a hozzátartozó egyedi jelszóval kell rendelkeznie, a Szövetség összes informatikai rendszeréhez. A felhasználónak ügyelnie kell arra, hogy a jelszót senki más ne ismerhesse meg.

A felhasználónév a következő névkonvenció alapján kerül meghatározásra, amennyiben az adott rendszerben megvalósítható: Vezetéknév + Keresztnév első betűje

5.9. Fizikai biztonság

5.9.1. Beléptetés

Biztosítani kell, hogy a Szövetség irodájába csak a megfelelő jogosultsággal rendelkezők léphessenek be, ennek érdekében minden munkavállaló névre szólóbelépőkártyával rendelkezik. Amennyiben a munkavállalóhoz vendég érkezik, az MRSZ irodájának területén a fogadójának kell a látogató felügyeletét biztosítania.

5.9.2. Szerverek biztonsága

A szerverterem fizikai biztonságát garantáló eszközöket rendszeresen ellenőrizni és karbantartani kell. A szerverek védelme érdekében a következő intézkedéseket kell meghozni:

- a helyiségben biztosítani kell a túlfeszültség elleni védelmet
- a szerverek számára a biztonságos leállást áramszünet esetén is biztosítani kell
- tűzjelző, páratartalom mérőt kell elhelyezni
- álpadlóval, álmennyezettel kell a szervertermet felszerelni
- tűzoltó berendezést kell elhelyezni a teremben

A szerverterembe kizárólag a megfelelő jogosultsággal rendelkező, az IT vezető által kijelölt személyek léphetnek be. A szerverteremben kizárólag szerverek tárolhatóak, ill. a szerverek üzemeltetésével szorosan összefüggő eszközök.

6. Felhasználói viselkedés

Az alábbi fejezetkben az információbiztonság felhasználói viselkedésre, elvárt magatartásra vonatkozó területek kerülnek kifejtésre.

6.1. Mobil eszközök kezelése

A Szövetség által biztosított mobil eszközök (lapot, telefon stb.) használatának alapelvei:

- A munkavállaló által használt céges mobilkészüléket az MRSZ biztosítja, annak tulajdonát képezi, így minden, a Szövetség által előírt ellenőrzés és korlátozás, amely a felhasználó által elfogadásra került érvényesíthető.
- Az érintett mobil eszköz abban az esetben csatlakoztatható a Szövetség infrastruktúrájához amennyiben:
    - Az eszközre tiltott alkalmazás nem került telepítésre (blacklist)

- PC vagy laptop esetén, az eszközön jogtiszta, a rendszergazda által telepített operációs rendszer fut
- Mobiltelefon esetén, az eszközön a gyártó által biztosított legfrissebb operációs rendszer fut
- A készülék zárolása / feloldása be van kapcsolva (pl.: PIN kód, ujjlenyomat)

A mobil eszköz kivihető szervezet logikai és fizikai infrastruktúrájából, de az eszköz biztonsága, integritása a felhasználó felelőssége marad az MRSZ irodákon kívül is.

6.2. E-mail/internethasználat

A Szövetség minden munkavállalójának saját, egyedi e-mail címet biztosít a Szövetség az alábbi névkonvenció alapján: *vezetéknév.keresztnév@hunvolley.hu.* A Szövetséghez tartozó e-mail cím magán célra korlátozottan használható, hivatalos, a munkavégzéshez kapcsolódó ügyek intézése pedig kizárólag ezen e-mail használatával megengedett.
Az e-mail klienshez csak a Szövetség által biztosított eszközökön keresztül lehet hozzáférni.
A Szövetség minden munkavállalója rendelkezik a munkavégzéshez használt eszközein internet hozzáféréssel. Ennek magán célra történő használata csak esetenként megengedett (pl. ügyintézés), annak figyelembevételével, hogy a biztonságos internethasználat a felhasználó felelőssége.

6.3. Biztonságtudatosság

A Szövetség biztonságtudatossági oktatásban részesíti az új belépőket az érkezéstől számított 3 hónapon belül, ami magában foglalja az alábbiakat:

- Jelen Szabályzat megismertetése és elfogadása
- az MRSZ tulajdonát képező eszközök kezelése
- személyes adatok kezelése
- jellemző támadások, típusai, kivédésük módszerei
- tiszta asztal, tiszta képernyő elve

6.4. Adathordozók kezelése

A felhasználók a Szövetség által biztosított gépekhez külső adathordozót csatlakoztathatnak, amennyiben az munkavégzésük szempontjából indokolt. Az adathordozók és adatok védelme a felhasználó felelőssége. Ennek érdekében az adathordozókat a használat idején kívül elzárva

kell tartani, másnak nem adható át. A felhasználónak kötelessége megbizonyosodni róla, hogy a másolni kívánt adatok megbízhatóak.
Amennyiben nem szükségesek továbbra az adatok, azokat visszaállíthatatlanul törölni kell.
Az eszköz biztonságosságának megállapításával illetve törlésével kapcsolatban szükség esetén az IT rendszergazda nyújt segítséget.

6.5. Tiszta asztal, tiszta képernyő

Minden dolgozó köteles a bizalmas iratokat elzárva tartani amint elhagyja a munkaállomását, laptopját. Az íróasztalon semmilyen, a Szövetség működésével kapcsolatos bizalmas dokumentáció nem tárolható felügyelet nélkül. Gondoskodni kell arról, hogy semmilyen nyomtatott dokumentum ne maradjon a fénymásolóban, nyomtatóban illetve fax berendezésekben.
A bizalmas információkat vagy személyes adatokat tartalmazó papír alapú dokumentumokat iratmegsemmisítő használatával kell megsemmisíteni amennyiben a továbbiakban nincs rá szükség.
A monitorokat úgy kell elhelyezni, hogy azokra minél kisebb rálátás essen, ezzel biztosítva, hogy idegen szemek számára a monitoron megjelenített tartalom nem látható. A munkaállomás őrizetlenül hagyásakor a felhasználó köteles zárolni a számítógépét (Windows + L) annak érdekében, hogy illetéktelenek ne tudjanak bizalmas információkhoz jutni a bejelentkezve hagyott számítógépen keresztül.

7. Üzemeltetés biztonsági szempontjai

7.1. Rendszerüzemeltetés

Az operációs rendszerekhez való adminisztrátori szintű hozzáférés csak a rendszergazda számára engedélyezett, kivéve, ha a főtitkár írásban engedélyezi más felhasználó számára is.
A rendszergazda feladata a Szövetség informatikai infrastruktúrájának üzemeltetése, a megbízható működés biztosítása. Gondoskodnia kell a rendszerek folyamatos biztonsági frissítéséről is.

7.2. Hálózatbiztonság

7.2.1. Szegmentáció

A Szövetség belső hálózatát az Internet irányából szegmentálva kell kialakítani.
Ez egyrészt szolgálja a belső rendszerek külső hálózatból történő elérését, valamint a belső hálózatról az internet elérését is.
A felhasználónak az internetelérés előtt a tűzfalon authentikálnia kell magát. Az authentikációnak a felhasználó számára teljesen transzparens módon az Internet böngésző segítségével, a Windows-os tartományi felhasználóval és jelszóval kell történnie.

Nem a Szövetséghez tartozó laptop, munkaállomás, telefon stb. nem csatlakozhat a Szövetség belső hálózatához (WiFi vagy fizikai hálózathoz). Logikailag elkülönített “vendég” Wifi hálózat létrehozható, ebben az esetben a Szövetséghez tartozó laptopokat, munkaállomásokat stb. technikailag korlátozni kell az ehhez való csatlakozásban.

7.2.2. Vezetéknélküli internetkapcsolat (Wifi)

Az MRSZ rendelkezik mind az alkalmazottak számára mind a vendégek számára fenntartott vezeték nélküli hálózati eléréssel, a kettő azonban teljesen szeparáltan működik.
A Szövetség belső WiFi hálózatában minimum az alábbi beállításokat kell alkalmaznia:

- MAC address szintű szűrés az engedélyezett eszközök számára

A vendég WiFi-n keresztül nem érhetőek el a céges erőforrások, az csupán az Internet elérését biztosítja.

7.2.3. Távoli elérés

A laptoppal rendelkező felhasználóknak lehetőségük van távolról elérni a Szövetség erőforrásait. Ehhez VPN (Virtual Private Network) megoldás használata kötelező. A VPN jogosultságot a standard jogosultságkezelési folyamaton keresztül lehet igényelni. A megfelelő technikai eszközökkel biztosítani kell, hogy VPN használata nélkül a Szövetség hálózata ne legyen távolról elérhető. A VPN csatlakozásra mindazon szabályok érvényesek, melyek a vállalati hálózatra való kapcsolódásra (kiemelten az engedélyezett eszközöket).

7.2.4. Titkosítás

Az adatok bizalmasságának, hitelességének és integritásának védelme érdekében az adatok továbbításakor vagy hordozásakor titkosítást kell alkalmazni az alábbi esetekben:

- különösen bizalmas információ;
- különleges személyes adatok kezelése

Ilyen információk továbbításakor a felhasználó felelőssége a megfelelő titkosítás. A megfelelő titkosítás elsősorban a következők használatát jelenti:

- - 7-Zip – csatolmányok tömörített formában való titkosítása, legalább 8 karakteres jelszóval
- - pendrive-ok esetében jelszóval kell védeni a hozzáférést

7.2.5. Vírusvédelem

A Szövetség tulajdonát képező minden eszköznek rendelkeznie kell vírusirtó programmal. Alapvető követelmények:

- Minden végpontot védő, egységes, automatikusan frissülő, központilag menedzselhető, automatikus riasztási és naplózási funkciókat teljesítő rendszer.
- Aktív vírusvédelemmel nem rendelkező kliens gépek esetében a hálózathoz való hozzáférés tiltása.
- A végfelhasználók nem módosíthatják, ill. kapcsolhatják ki a vírusvédelmi szoftvert a saját eszközükön, ezt technikailag korlátozni kell.

7.2.6. Tűzfal

A tűzfalak és határvédelmi eszközökben, rendszerben történő módosításokat naplózni kell, és minden módosítás után le kell menteni az aktuális konfigurációs állományokat. Minden évben az IT működésért felelős vezetőnek felül kell vizsgálni a konfigurációkat, és jóvá kell hagynia.

7.3. Adatok mentése

7.3.1. Mentési folyamatok

A Szövetség meghatározza és dokumentálja az üzletmenet szempontjából kritikus és közepesen kritikus rendszereket (lásd: 18.1-es fejezet), majd ezekre a rendszerekre a rendszerek biztonsági specifikációjában meghatározottan, de legalább az alábbi módon és rendszerességgel kell biztonsági mentéseket végrehajtani:

- Napi szinten inkrementális mentés
- Hetente teljes mentés
- Legalább 1 évre visszamenőleg tárolni kell

Gondoskodni kell arról, hogy a mentések bármikor visszaállíthatók legyenek, ezzel biztosítva, hogy az adatvesztési kockázat a lehető legkisebb mértékű legyen. A mentéseket az éles szerverektől elkülönítve, külön helyiségben kell tárolni.

7.3.2. Visszatöltési eljárások, tesztek

A 7.3.1. pontban meghatározott mentésekkel évente visszaállítási tesztet kell végrehajtani. A minta alapú tesztelés elfogadott módszer, ennek értelmében egy tesztelési folyamat során nem kell minden alkalmazás és rendszer visszaállítását tesztelni, azonban a mentési felelős felelőssége, hogy a magas besorolású rendszerek és alkalmazások tesztje évente megtörténjen. A mentések kezelésével kapcsolatban nyilván kell tartani azon személyes adatokat, amelyeknek törlése szükségessé vált és a visszaállítás során ezen adatok visszatöltését meg kell akadályozni. Amennyiben erre a rendszer nem képes, akkor a visszaállítás után törölni kell

ezeket az adatokat. A feladat elvégezhető automatizált módszerrel, de mentési felelős felelőssége, hogy ezen adatok ne kerüljenek visszaállításra.

7.4. Naplózás

A számonkérhetőség és az auditálhatóság biztosítása érdekében a rendszerekben biztosítani kell a tevékenységek naplózását, mely biztosítja a fontosabb események utólagos kivizsgálását, különös tekintettel azokra, melyek a rendszer biztonságát érintik. A naplóállományokat időszakosan felül kell vizsgálni a rendszer felelőse által, kiemelt hangsúlyt fektetve a módosító illetve törlő tevékenységek felülvizsgálatára.
A naplózásnak ki kell térni legalább az alábbi tevékenységekre:

- Belépés / kilépés
- Adminisztrátori bejelentkezés
- Műveletek amik admin jogot kívánnak
- Rendszerüzenetek (újraindítás, leállítás stb.)
- Adatmódosítás, adattörlés, különös tekintettel a személyes adatokra

A naplónak tartalmaznia kell legalább az alábbiakat:

- felhasználónév
- dátum, idő
- elvégzett tevékenység

A naplókhoz a rendszer üzemeltetője és az MRSZ rendszergazdája, valamint főtitkára férhet hozzá és a fájlokat legalább 3 hónapig meg kell őrizni.

7.5. Szoftverek

Az rendszergazda kötelessége, hogy naprakész hardver- és szoftvernyilvántartást vezessen az MRSZ tulajdonában lévő minden telepített informatikai eszközről. A Szövetségnek rendelkeznie kell egy szoftver katalógussal, illetve egy szoftver listával, ami definiálja a felhasználók által telepíthető és használható szoftvereket. A szoftverlistában nem szereplő alkalmazások telepítése előzetes vizsgálathoz és a rendszergazda engedélyéhez kötött. Csak a munkavégzéshez szükséges szoftverek telepíthetők. Kizárólag jogtiszta szoftverek használhatóak.
Szoftverek telepítése csak adminisztrátori jogkörrel rendelkező felhasználók számára lehetséges.

7.6. Kiszervezett tevékenységek

Harmadik fél által végzett tevékenységek (pl. üzemeltetés) esetén a szerződésnek tartalmaznia kell az alábbi elemeket:

- meghatározott SLA-k
- a szolgáltatónak biztosítania kell, hogy minden szükséges licensz rendelkezésére áll
- a tárolt adatok tulajdonjoga
- a rendszerhez való hozzáféréseket
- incidenskezelési alapelveket és értesítési kötelezettségeket
- adatvédelmi alapelveket

8. Fejlesztés

8.1. Környezetek szétválasztása

Fejlesztői-, teszt- és éles környezeteket szét kell választani. Az egyes környezetek között adatforgalom csak a rendszergazda jóváhagyást követően, dokumentáltan lehetséges.
A fejlesztői- és teszt környezetekben nem szerepelhetnek aktív, éles adatok. Éles rendszerből adatok kizárólag anonimizálást követően vihetők át. Tesztelés nem végezhető valós személyes adatokon.

8.2. Fejlesztési folyamat

Amennyiben a Szövetség által használt valamely rendszerben fejlesztés szükséges, az a Főtitkár vagy delegáltja jóváhagyásával lehetséges. Az elkészült módosításokat minden esetben teszt rendszerben kell tesztelni az élesbe állítás előtt. Mind felhasználói funkcionális tesztet, mind informatikai biztonsági tesztet végezni kell az igénylő felhasználó illetve a rendszergazda által. A fejlesztési igényt, tesztelési eredményeket és a go live döntést dokumentálni kell.

9. Adatkezelés

9.1. Adatok megőrzési ideje

Az adatok megőrzési idejét az MRSZ adatvagyonleltára tartalmazza. Gondoskodni kell arról, hogy az adatok a megőrzési idő lejárta után törlésre kerüljenek. A törlési folyamatot a 23. pont tartalmazza.

9.2. Adatok törlése

A tárolt adatokat a megőrzési idő végén, vagy személyes adatok esetében az adatalany kérésére, illetve megfelelő jogalap hiányában törölni kell. A megőrzési idők nyilvántartása az adatgazda felelőssége. A törlési folyamat során biztosítani kell, hogy az adatok véglegesen törlődjenek, visszaállításuk ne legyen lehetséges.
Az adatok törlését két fajta folyamat indíthatja el: automatikus vagy ad-hoc kérés.

9.2.1. Automatikus

Amennyiben egy személyes adatnak lejár a megőrzési ideje, a törlési folyamat automatikus megindul.
Az adatgazda listát készít a törlendő adatokról, majd azt a főtitkár jóváhagyása után eljuttatja a rendszer üzemeltetőjéhez, aki végrehajtja a törlést. A törlés tényét dokumentálni szükséges.
Az adatgazdának meg kell győződnie róla, hogy a több helyen is tárolt adatokat minden helyről törölték.

9.2.2. Ad-hoc törlés

Amennyiben egy adatalany törlési kérést indít a Szövetség felé, a kérés jogosságának megvizsgálása után a Szövetség elindítja a törlési folyamatot. Tipikusan hozzájárulás alapú adatkezelések tartozhatnak ide.
A kérés jogosságát és jogalapját a Szövetség 8 napon belül megvizsgálja, amennyiben teljesíthető a kérés, minél hamarabb, de maximum 30 napon belül teljesíti a Szövetség.

9.3. Adatkinyerés

Biztosítani kell, hogy a Szövetség által használt rendszerekből az adatok kinyerhetőek legyenek, széles körben elterjedt gépileg olvasható formátumban (pl. .xls, ..pdf, .doc). Az adatkinyerésre vonatkozó igényeket a hunvolley@hunvolley.hu e-mail címen keresztül kezeli a Szövetség, amit elérhetővé kell tenni az adatalanyok számára. Az adatalanyok jogai részletesen az Adatkezelési Szabályzatban találhatóak.
Az adatok kinyerésére érkező kérést a Szövetség ellenőrzi, majd ha megállapította a jogosságát a Főtitkár értesítésével továbbítja a rendszer üzemeltetője számára, aki elvégzi az exportálást.
Az ellenőrzés során meg kell győződni az igénylő személyazonosságáról.
A folyamat során minden esetben dokumentálni kell az alábbiakat:

- a beérkező kérés dátuma
- az igénylő neve, elérhetősége
- igényelt adatok köre
- igény teljesítésének dátuma
- igény teljesítője

A dokumentációt elektronikusan 5évig meg kell őrizni, ahhoz az Szövetség főtitkára és operatív igazgatója férhet hozzá.
A kinyert adatok tárolása és továbbítása során biztosítani kell az adatok eredeti biztonsági szintjének megvalósulását.

9.4. Adatgazdák feladatai, felelősségei

Az adatvagyonleltárban szereplő vagyonelemek mindegyikéhez formális adatgazda meghatározása szükséges. Az adatgazdákat a mindenkori Főtitkár nevezi ki e-mailes formában, egy évre. A kinevezés korlátlan ideig meghosszabbítható.
Az adatgazda feladata a kezelt adatok biztonsági osztályba sorolása (lásd: 26. Fejezet) és az ennek megfelelő biztonsági intézkedések meghatározása (hozzáférések korlátozása, törlések biztosítása stb.).

9.5. Információk osztályozása

9.5.1. Adatkategóriák

Az adatok kockázattal arányos védelme érdekében azokat kategóriákba szükséges sorolni, melyek meghatározzák a szükséges védelmi szintet. A Szövetség a következő adatkategóriákat használja:

Nyilvános - Bárki számára hozzáférhető az MRSZ által önkéntesen nyilvánosságra hozott adat, melynek megismerése nem sérti az egyéb adatkategóriákhoz kapcsolható védendő érdekeket, és nem sorolható a további kategóriák egyike alá sem.

Üzleti, de nem nyilvános - Mindazon adat, ami akár a Ptk., akár a Bit. szerint üzleti titoknak minősül. Bizalmas kezelése stratégiai fontosságú az üzleti vállalkozás szempontjából.

Személyes - Mindazon adat, amely az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. Törvény értelmében személyes adatnak minősül.

Kiemelten védett - Kiemelt adatnak tekinti a Szövetség mindazon adatot, amely az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény értelmében különleges adatnak minősül, így különösen az egészségügyi adatot.

10. Információbiztonsági adminisztratív folyamatok

10.1. Üzletmenet folytonosság – BCP, DRP

A Szövetségnek rendelkeznie kell Üzletmenet folytonossági (BCP) és Katasztrófa helyreállítási (DRP) tervekkel. Ezeket a terveket külön dokumentumban alkotja meg a Szövetség, felelőse Farkas Gábor.

10.1.1. A tervek tesztelése

Az elkészített BCP és DRP tervek megvalósíthatóságát és alkalmazhatóságát 2 évente tesztelni szükséges.

Az elkészített BCP és DRP terveket évente felül kell vizsgálni. Felelőse: Farkas Gábor.

10.2. Incidensmenedzsment

A hatékony védelem érdekében kiemelten fontos az esetleges információbiztonságot, adatvédelmet vagy üzletmenet folytonosságot (beleértve IT üzemeltetés is) események észlelése, elemzése, és az esetleges incidensek kezelése, eszkalálása.

10.2.1. Incidensek észlelése

Az információbiztonsági incidensek észlelése történhet a monitoring eszközök automatikus értesítése, vagy bejelentés által.
A bejelentés érkezhet a szervezeten belülről vagy kívülről is. Az incidenseket és lehetséges incidenseket az alábbi e-mail címen kell bejelenteni: farkas.gabor@hunvolley.hu. A bejelentésnek tartalmaznia kell az incidens helyét és idejét, az érintett adatok körét, valamint a bejelentő nevét és elérhetőségét.

10.2.2. Incidensek kezelése

A kijelölt incidensmenedzser feladata az észlelt incidens megoldójának meghatározása, a megoldási folyamat nyomonkövetése, szükség esetén több terület (pl. pénzügy) bevonása.
Az észlelést követően az incidenst az alábbi táblázat szerint be kell sorolni a megfelelő osztályba:

Kategória	*Definíció*
4 – Alacsony	Minimális hatás a szervezetre vagy a szolgáltatás elérhetőségére. Nincs sérült információ. Minimális helyreállítási költség és idő.
3 – Közepes	Kritikus szolgáltatások működnek, de csökkent hatékonysággal. Kismértékű, nem szenzitív adat (pl. Cégadatok) elvesztek, kiszivárogtak vagy módosultak. Alacsony helyreállítási költség és idő.
2 – Magas	A felhasználók akár 30%-a tapasztal kiesést kritikus szolgáltatásokban. Korlátozott hozzáférésű Cégadatok elvesztek, kiszivárogtak vagy módosultak. A kibertámadás a szolgáltatások funkcionalitásának 15%-át érinti. Mérsékelt helyreállítási költség és idő.

1 – Kritikus	A felhasználók akár 60%-a tapasztal kiesést kritikus szolgáltatásokban. Személyes adat, érzékeny adat (bizalmas Cégadat, szigorúan bizalmas Cégadat) elveszett, kiszivárgott vagy módosult, vagy az adatvesztés mértéke ismeretlen. A kibertámadás a szolgáltatások funkcionalitásának 50%-át érinti. Jelentős helyreállítási költség és/vagy idő. Továbbá minden adatvédelmi incidenst kritikusnak kell minősíteni alapértelmezetten.

Személyes adatok megsértése esetén az incidensmenedzsernek a Főtitkár bevonásával 72 órán belül értesítenie kell a Felügyelő hatóságokat. Amennyiben az értesítés a hatóságok felé nem történt meg 72 órán belül, a késedelem okát mellékelni kell. A jelentésnek legalább a következő adatokat kell tartalmaznia (az információkat részletekben is meg lehet adni, indokolatlan késedelem nélkül):

- Leírás a személyes adatok megsértésének természetéről (az érintettek kategóriája és hozzávetőleges száma, valamint a személyes adatok kategóriája és hozzávetőleges száma).
- Az adatvédelmi tisztségviselő vagy más kapcsolattartó neve és elérhetősége, akitől további információ gyűjthető.
- Lehetséges következményei az adatok megsértésének.
- Az adatkezelő által a személyes adatok megsértésének kezelése érdekében tett vagy javasolt intézkedések (a lehetséges káros hatások mérséklésére irányuló intézkedések).

Amennyiben a személyes adatok megsértése magas kockázatot jelenthet a természetes személyek jogaira és szabadságára nézve, az adatok megsértését kommunikálnia kell az incidensmenedzsernek az érintettek számára is, indokolatlan késedelem nélkül. A közleménynek tartalmaznia kell a felügyelő hatóság számára biztosított adatokat, egyértelműen érthető formában.

Ez a közlemény nem kötelező, ha:

- Megfelelő technikai és szervezeti védelmi intézkedéseket hajtottak végre és ezeket az intézkedéseket alkalmazták az érintett személyes adatokon, különösen azokat, amik a személyes adatokat érthetetlenné teszik minden olyan személy számára, aki nem rendelkezik megfelelő jogosultsággal, például titkosítás.
- Utólagos intézkedéseket hajtottak végre, ami biztosítja, hogy az érintettek jogainak vagy szabadságának sérülésének a kockázata már nem valószínűsíthető.
- Aránytalan erőfeszítést igényelne. (Ebben az esetben nyilvános közlemény vagy hasonló intézkedés szükséges, amellyel az érintetteket ugyanolyan hatékony módon tájékoztatják.)

- Ilyen esetekben a feldolgozást megelőzően adatvédelmi hatásvizsgálatot kell végezni annak érdekében, hogy értékelni lehessen a magas kockázat valószínűségét és súlyosságát, figyelembe véve a feldolgozás jellegét, terjedelmét, kontextusát és célját, valamint a kockázat forrásait. A hatásvizsgálatnak ki kell terjednie különösen a kockázat enyhítésére, a személyes adatok védelmének biztosítására tervezett intézkedésekre, biztosítékokra és mechanizmusokra.

10.2.3. Incidensek dokumentálása

Az észlelt incidenseket minden esetben dokumentálni kell. A dokumentációnak legalább a következőket kell tartalmaznia:

- az incidens helye és ideje
- a bejelentő neve és elérhetősége
- az incidens jellege
- az incidens osztályozása
- a megoldásért felelős személy
- az érintett adatok köre
- az incidens megoldása

A dokumentációt elektronikus formában (xls, doc.) a Szövetség fájlszerverén legalább 5 évig meg kell őrizni.

10.2.4. Incidensek elemzése, tanulságok levonása

Az incidens megoldását követő két héten belül elemzést kell készíteni, amiben megvizsgálják az incidens okát és következményeit, valamint a végrehajtott intézkedések hatékonyságát.
Az elemzés segítségével levont következtetéseket és tanulságokat dokumentálni kell.

11. Kockázatelemzés

A Szövetség információbiztonsági kockázatelemzést végez, amivel elősegíti az adatok és rendszerek kockázatokkal arányos védelmét. A kockázatelemzés eredményeit nyomon követi, a feltárt hiányosságokat javítja.

11.1. Rendszerek osztályozása

A Szövetség a kockázatelemzés előtt osztályozza a rendszereit, kritikusság szerint. Az alábbi osztályozás használható:
„A” osztály – Kritikus, a Szövetség működéséhez elengedhetetlen rendszer. Nagy mennyiségű személyes és üzleti adatot tartalmaz
„B” osztály – Közepesen kritikus, a Szövetség működéséhez fontos rendszer. Tartalmaz személyes adatot és üzleti információt.

„C” osztály – Nem kritikus alkalmazás. Kiesése nem befolyásolja a Szövetség működését (pl. Skype)

11.2. Kockázatelemzés elvégzése

Az adatok és információk védelme érdekében a Szövetség informatikai kockázatelemzést végez. Ennek során:

- azonosítja a Szövetség információ biztonságát, rendszereit, infrastruktúráját fenyegető veszélyeket
- elemzi a veszélyek bekövetkezési valószínűségét és hatását
- meghatározza a kockázatot
- akciótervet dolgoz ki a maradványkockázatok csökkentésére

A Szövetség az információbiztonsági kockázatelemzést legalább kétévente elvégezteti. A mindenkori operatív igazgatónak felelőssége meghatározni:

- A kockázatelemzés terjedelmét
- A kockázatelemzés végzőjét

Az operatív igazgató felelősség az akcióterv jóváhagyása és nyomon követése.

12. Felülvizsgálat

A Szabályzatot évente legalább egy alkalommal felül kell vizsgálni. A felülvizsgálatot a mindenkor Főtitkárnak kell jóváhagynia.

Változtatás Új elvárás beépítése / Felülvizsgálat / Átdolgozás	**Változtatás helye**	**Rövid leírás**	**Jóváhagyás dátuma**
-	**-**	-	dátum