Magyar Honvédség
Budapesti Nyugállományúak Klubja
1143 Budapest, Stefánia út 34.
honlap: www.bpnyklub.hu
e-mail: bpnyklub@bpnyklub.hu

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

2018.

Tartalomjegyzék

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja

A Szabályzat alapvető célja, hogy az elektronikus információs rendszerek (a továbbiakban: rendszer, rendszerek) használata, alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. Meghatározza a biztonságos üzemeltetés alapvető szabályait, az ellenőrizhető informatikai környezet kialakításához szükséges feltételeket, a használathoz és üzemeltetéshez kapcsolódó magas szintű szabályokat, az alapvető biztonsági normákat és követelményeket.

A Szabályzat előmozdítja az informatikai és kommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, ezzel támogatva, hogy a KLUB által kezelt információvagyon sértetlensége, bizalmassága és rendelkezésre állása biztosított legyen.

A Szabályzat rögzíti a rendszerekre és a rendszerekkel kapcsolatos tevékenységekre vonatkozó adminisztratív, fizikai és logikai követelmények teljesítésével összefüggő feladatokat, folyamatokat és felelősségeket.

2. A Szabályzat hatálya

Jelen Szabályzat személyi hatálya kiterjed az MH Budapesti Nyugállományúak Klubja (a továbbiakban KLUB) valamennyi tagjára, informatikai szolgáltatásait használó felhasználókra és rendszergazdákra, tárgyi hatálya kiterjed a KLUB teljes infrastruktúrájára, azaz a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére, a folyamatokra, a székhelyre és valamennyi telephelyre és a létesítményekre is. Fel-használónak minősülnek a KLUB tagjai.

A Szabályzatot az alábbiakban felsorolt jogszabályokkal összhangban kell alkalmazni:

a) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.),

b) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.),

c) az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet.

3. Értelmező rendelkezések

1. **Adatbiztonság**: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

2. **Adatfeldolgozás**: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.

3. **Adatfeldolgozó**: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.

4. **Adatfelelős**: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzé teendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

5. **Adatgazda**: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

6. **Adatkezelés**: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése.

7. **Adatkezelő**: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza, valamint végrehajtja (vagy az általa megbízott adatfeldolgozóval végrehajtatja).

8. **Asztali munkaállomás**: a felhasználó rendelkezésére bocsátott számítástechnikai eszköz, mely alapvetően a számítógépből, monitorból, billentyűzetből és egérből, illetve más csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, nyomtató stb.) állhat.

9. **Bizalmasság**: az információ azon jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára titok. A bizalmasság elvesztését felfedésnek nevezzük, mely esetén a bizalmas információ arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.

10. **Biztonság**: az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősíti.

11. **Biztonsági esemény**: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

12. **Biztonsági esemény kezelése**: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

13. **Domain név**: tartománynév (műszaki azonosító), amelyet elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen cím tartományok (IP címek) helyett használnak. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek azonosítására szolgáló névtartomány (például: bpnyklub.hu).

14. **Elektronikus információs rendszer (EIR):** az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese (Ibtv. 1. § 14. b).

15. **Felhasználó**: az a természetes személy, aki a KLUB informatikai infrastruktúrát használja.

16. **Hitelesség**: az információ akkor hiteles, ha az elvárt, hozzáértő, megbízható forrásból származik.

17. **Informatikai erőforrások**: a hardver, szoftver eszközök összessége.

18. **Internet**: a világháló.

19. **Közérdekű adat**: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv, vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől.

20. **Közérdekből nyilvános adat**: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

21. **Mobil eszközök**: notebook, netbook, tablet, palmtop, okos telefon.

22. **Okos telefon**: internetezésre és/vagy dokumentumkezelésre is használható mobil telefon.

23. **Rendelkezésre állás**: annak biztosítása, hogy a szükséges információ a szükséges időben az arra jogosultak számára meghatározott formában hozzáférhető, elérhető legyen.

24. **Rendszergazda:** hálózati szolgáltatást nyújtó számítógép adminisztrátora.

25. **Sértetlenség**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének meg-felelően használható;

26. **Tűzfal**: olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.

27. **Végfelhasználói eszköz**: minden olyan informatikai eszköz, amely nem a központi rendszerek működtetésére használt eszköz.

28. **WEB adminisztrátor**: a KLUB web szerverét működtető, vagy a KLUB honlapjának felügyeletét ellátó személy. A webes adat- és tartalomszolgáltatást a KLUB tagozataiból és az ügyvezetésből kijelölt felelősök végzik.

4. Alapelvek

A rendszerekkel, infokommunikációs eszközökkel és adathordozókkal kapcsolatos fejlesztői, üzemeltetői, biztonsági, továbbá felhasználói tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, üzemeltetési és védelmi előírásokat úgy kell meghatározni és dokumentálni, hogy azok garantálják az információbiztonság szükséges és elégséges szintjét.

Az Ibtv. 5. §-a alapján az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

Kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni.

A fenti tevékenységek szabályozását úgy kell kialakítani, hogy a tevékenységek megtervezéséért és végrehajtásáért való felelősséget minden esetben meg lehessen állapítani.

5. A szabályozás rendszere

Jelen szabályzat az informatikai biztonsági szabályozás alapdokumentuma, amely átfogóan és keretjelleggel szabályozza az információbiztonsági szempontból releváns kérdéseket, területeket a I./2. (2) bekezdésében felsorolt jogszabályi előírásoknak, követelményeknek megfelelően. A szabályzatot a KLUB titkára készíti el és gondozza.

6. Információbiztonsági kockázatfelmérés és –kezelés

A KLUB működése során használt rendszerek esetében a kockázatfelmérést szabványok és jogszabályok e paragrafusban hivatkozott dokumentumok alapján kidolgozott, elektronikus információs rendszerek kockázatkezelési szabályzata határozza meg.

A kockázatkezelési szabályzat egyértelműen tartalmazza:

a) kockázatok azonosítás szabályait,
b) fenyegetéseket,
c) védelmi intézkedéseket,
d) sebezhetőségeket,
e) hatások, következmények azonosítását,
f) kockázatok becslését, kockázatértékelést,
g) kockázatkezelést,
h) az információbiztonsági kockázatok monitorozását és felülvizsgálatát.

A kockázatfelmérést követő kockázatkezelésre vonatkozó javaslatokat a kockázat kezelési tervet a KLUB elnökének bevonásával az elektronikus információs rendszerek biztonságáért felelős személy állítja össze.

A KLUB elnöke által jóváhagyott kockázatkezelési terv végrehajtásáról az érintett szakterületek gondoskodnak.

7. A védelmi intézkedések

A rendszerhez rendelt védelmi intézkedések tervezése és teljesítése az Elektronikus információs rendszerek 2. (3) bekezdésében felsorolt jogszabályi előírásoknak, követelményeknek megfelelően és a kockázatkezelési szabályzata alapján történik.

A működés során használt rendszerek esetében a még meg nem valósított vagy részlegesen megvalósított védelmi intézkedések teljesítésének tervezése a rendelkezésre álló erőforrások figyelembe vételével történik.

II. FEJEZET
ELLENŐRZÉS ÉS ÉRTÉKELÉS

1. Az ellenőrzés végrehajtása

Az ellenőrzést végezhetik:

a) a KLUB Felügyelő bizottsága,

b) a KLUB elnöke által kijelölt bizottság,

c) illetékes hatóság.

A végrehajtott ellenőrzést a jelen Szabályzat mellékleteként kiadott ellenőrzési naplóban rögzíteni kell:

a) végrehajtójának nevét,

b) megállapításait,

c) a megállapítások alapján készített intézkedési terv adatait (készítő, jóváhagyó, végrehajtási határidők),

Nem ellenőrizhető a személyes adatokat tartalmazó adatállomány.

III. FEJEZET
AZ INFORMATIKAI BIZTONSÁG SZERVEZETE

1. A KLUB elnöke

a) felelős a KLUB informatikai tevékenységének jogszerűségért, beleértve az informatikai biztonsági tevékenységet,

b) gondoskodik az informatikai biztonság személyi és tárgyi feltételeinek biztosításáról,

c) gondoskodik – szabályozás és ellenőrzés útján – az Ibtv.-ben és a kapcsolódó jogszabályokban előírt, információbiztonsággal összefüggő tevékenységek végrehajtásáról,

d) informatikai biztonsági kérdésekben dönt,

e) közreműködik – az informatikai biztonsági szempontok meghatározásával – az informatikai biztonsággal összefüggő informatikai szakmai döntések előkészítésében.

2. A KLUB titkára

a) gondoskodik a rendszerek és a bennük kezelt, feldolgozott, tárolt adatok zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosításához szükséges intézkedések megtervezése, megvalósítása, ellenőrzése és szükséges korrekciója érdekében szükséges feladatok végrehajtásáról,

b) felelős – hatáskörük keretein belül – az irányítása alá tartozó szervezeti egységek által üzemeltetett vagy fejlesztett rendszerek jogszerű és szakszerű működéséért, működtetéséért, a rendszerekre vonatkozó informatikai szakmai és információbiztonsági előírások teljesítéséért, a hatályos belső szabályzatok és a bevált gyakorlatok érvényesítéséért,

c) kezdeményezi az irányítása alá tartozó szervezeti egységek tevékenységével érintett rendszerekkel összefüggő informatikai szakmai és információbiztonsági intézkedéseket, beszerzéseket, illetve közreműködik azok végrehajtásában,

d) az informatikai biztonsággal összefüggő ellenőrzéseket tervez és hajt végre, illetve gondoskodik az ellenőrzések lefolytatásáról,

e) az informatikai biztonság megsértésének észlelése esetén kivizsgálja a megsértés körülményeit és – az elnök útján – javaslatot tesz az érintett szervezeti egység vezetőjének a megteendő intézkedésekre.

3. A rendszer működtetéséért felelős szervezeti egység vezetője, az adatgazda

A rendszer működtetéséért felelős szervezeti egység vezetője, az adatgazda

a) felelős a rendszer használatára vonatkozó szakmai szabályok meghatározásáért és írásbeli rögzítéséért, beleértve a – hatáskörébe tartozó – tervezési és szabályozási feladatokat is,

b) ellátja a rendszer használatához szükséges jogosultságok kezelésével kapcsolatos, számára meghatározott – irányítói – feladatokat,

c) meghatározza a rendszer által kezelt, feldolgozott, tárolt adatok körét, típusát, őrzési idejét,

d) javaslatot tesz a rendszer fejlesztésére, módosítására, kivonására.

Az elektronikus információs rendszer biztonságáért felelős személy az elektronikus információs rendszerét érintő biztonsági eseményről az Ibtv.-ben meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

IV. FEJEZET
AZ INFORMATIKAI BIZTONSÁG VESZÉLYEZTETÉSE, MEGSÉRTÉSE

A Szabályzat, a vonatkozó jogszabályok, belső szabályzatok be nem tartása, valamint az informatikai biztonság veszélyeztetése, megsértése esetén a felhasználóval szemben fegyelmi, illetve büntetőjogi felelősségre vonásnak lehet helye.

V. FEJEZET
SZERVEZETI BIZTONSÁGI KÖVETELMÉNYEK

1. Helyettesítés

Az informatikai és az informatikai biztonsági szerepkörök és feladatok személyre telepítésekor a közvetlen vezető köteles gondoskodni a helyettesítésről.

VI. FEJEZET
SZEMÉLYI BIZTONSÁGI KÖVETELMÉNYEK

A jogtalan hozzáférés, információvesztés és rongálás elkerülése érdekében alkalmazni kell a „tisztaasztal, tisztaképernyő”szabályt, azaz az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat. Külön figyelmet kell fordítani és messzemenően be kell tartani az információk/adatok minősítésére vonatkozó előírásokat.

A nyomtatókról azonnal el kell távolítani a kinyomtatott iratokat.

Az aktuálisan nem használt számítógépet ki kell kapcsolni vagy jelszóvédetten zárolni.

1. Információbiztonsági képzés, továbbképzés

A KLUB munkatársait, szakmai felelősöket a KLUB-nál végzendő tevékenység megkezdésekor vagy legkésőbb 3 hónapon belül a Szabályzat tartalmát megismertető, a biztonsági események jelentési kötelezettségére is figyelmeztető, továbbá az információbiztonsági tudatosság növelését is célzó képzésben kell részesíteni.

Az információbiztonságra vonatkozó jogszabályi környezet megváltozásakor, továbbá ha a KLUB informatikai biztonságát, illetve a jelen

Szabályzat tartalmát érintő jelentős változás következik be, a jogszabályváltozás hatályba lépését, illetve a jelentős változást követő 60 napon belül a munkatársakat információbiztonsági továbbképzésben kell részesíteni.

VII. FEJEZET
INFORMATIKAI BIZTONSÁGI FELADATOK ÉS FELELŐSSÉGEK MEGHATÁROZÁSA

1. Informatikai biztonsági feladatok

a) A rendszerbe állításra tervezett új informatikai és kommunikációs eszközök, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról, illetve az elavultak kivonásáról.

b) A felhasználók részéről felmerült, az alapvető irodai informatikai és kommunikációs eszközökön és rendszereken túli igények elbírálása, a jogos igények lehetőség szerinti kielégítése, az adott szakterület vezetőjével egyeztetve javaslattétel az adott feladat ellátására alkalmas más eszköz, rendszer használatára.

c) A felhasználók személyi számítógépeinek (asztali és hordozható gépek) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása, működési zavar, meghibásodás, rendellenes működés esetén a hibaelhárítás lehető leggyorsabb megkezdése.

d) Szankciók alkalmazása a biztonsági előírásokat megsértő felhasználókkal szemben és a szankciókkal sújtott felhasználók haladéktalan tájékoztatása. Az alkalmazott szankciókról tájékoztatni kell a munkahelyi vezetőt. Tekintettel arra, hogy a szabályok megszegése az egész KLUB informatikai rendszerének, s így mások munkájának biztonságát is veszélyeztetheti.

e) A kommunikációs rendszerek viszonylatában a jogszabályokban meghatározott nyilvántartások, naplók vezetése, amelyeket a jogszabályokban meghatározott esetekben, törvényes megkeresés alapján az illetékes hatóságoknak kiszolgáltat.

f) Az általános informatikai ismereteken túli, az adott szolgáltatás igénybevételéhez szükséges ismeretek nyújtása.

g) A vezető az informatikai biztonsági előírások megsértésnek észlelése esetén köteles:

- azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében,
- amennyiben meghatározható rendszerre korlátozódik a biztonsági előírások megsértése, indokolt esetben kezdeményezni a rendszer használatának felfüggesztését.

- kivizsgáltatni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,
- a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni.

2. A felhasználó jogai és kötelezettségei:

a) A felhasználó jogosult a munkavégzéshez szükséges infokommunikációs eszközöket használni, a használatukhoz szükséges ismereteket dokumentáció vagy oktatás formájában megkapni.

b) A munkavégzéshez szükségesnek ítélt eszközök, szoftverek beszerzését, telepítését igényelni,

c) A felhasználó a rendelkezésére bocsátott infokommunikációs eszközöket csak a KLUB céljaival, feladataival kapcsolatos, a munkaköri feladatai ellátásához szükséges tevékenység céljára, rendeltetésszerűen, a számára megállapított jogosultságok keretein belül, rendeltetésszerűen használhatja.

d) A Hálózatra bármilyen berendezést (különösen: számítógépeket, perifériákat – nyomtató, scanner külső adattárolók - fax, okostelefon, stb.) csak a Honvéd Kulturális Központ rendszergazdájának engedélyével szabad csatlakoztatni. Ha az eszköz adattárolásra is alkalmas, akkor a csatlakoztatás után vírusellenőrzést kell végrehajtani, illetve az adatok tárolására vonatkozó jelen és más vonatkozó szabályzatok és előírások betartására különös figyelmet kell fordítani

e) A felhasználó köteles a használatra átvett informatikai eszközöket az elvárható gondossággal kezelni és a károsodásoktól védeni.

f) A felhasználó személyes anyagi felelősséggel tartozik az általa szándékosan vagy gondatlanságból (pl. nem rendeltetésszerű használattal) az infokommunikációs eszközökben okozott bizonyított károkért.

g) A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tevékenységért, tranzakcióért a bejelentkezéstől a kijelentkezésig a felhasználó felelős. Ez a felelősség akkor is fennáll, ha a tevékenységet, tranzakciót harmadik személy hajtotta végre, amennyiben erre a Szabályzat előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.

h) A munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, jelszavas képernyőkímélővel védeni, illetve ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni, vagy azt kikapcsolni, amennyiben azt felügyelet nélkül hagyja. A munkaállomást a munkaidő végén vagy a munkavégzés befejezésekor – eltérő rendelkezés hiányában – ki kell kapcsolni.

i) Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó

programból, a felhasználói fiókból és az azonosított kapcsolatból is kijelentkezett.

j) Azt a munkaállomást, infokommunikációs eszközt, amelybe privilegizált rendszeradminisztrátor jogosultsággal jelentkeztek be, személyes felügyelet nélkül hagyni tilos.

k) A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott dokumentumhoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott dokumentumot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

l) A felhasználó a rendelkezésére bocsátott mobil infokommunikációs eszközöket és adathordozókat köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

m) A felhasználó köteles az általa észlelt informatikai biztonsági eseményről vagy annak bekövetkezési lehetőségéről értesíteni közvetlen vezetőjét. A felhasználó köteles a saját feladatkörében nem megoldható informatikai biztonsági problémáról, hiányosságról értesíteni közvetlen vezetőjét vagy a feladatkörrel rendelkező, kijelölt személyt, és közreműködni a szükséges intézkedések végrehajtásában.

n) A felhasználó köteles meghibásodás, üzemzavar észlelésekor, vírusfertőzés (vagy annak gyanúja) esetén haladéktalanul értesíteni a KLUB titkárát, a számítógép további használatát a titkár intézkedéséig felfüggeszteni. A hibaelhárítás folyamán a szakemberekkel együttműködni, számukra a szükséges információkat megadni.

3. A meg nem engedett tevékenységek szankciói

Jelen Szabályzat megsértésének gyanúja esetén a cselekményt ki kell vizsgálni, és a vizsgálatra a Elnök által megbízott legalább három tagú felelős (kivizsgáló) bizottságnak javaslatot kell tennie a megbízónak a szükséges intézkedésekre, amelyekre a következők az irányadók:

a) A Szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.

b) A Szabályzat ismételt megszegése szándékos elkövetésnek minősül.

c) A Szabályzat szándékos megsértése esetén az elkövető a Hálózat használatából ideiglenesen vagy véglegesen kizárható,és az eset súlyosságától függően eljárás lefolytatása kezdeményezhető ellene.

d) A szándékos elkövető – a fentieken túl, amennyiben kimutatható anyagi kár is keletkezett - köteles megtéríteni az általa okozott károkat a vonatkozó jogszabályok és más közjogi szervezetszabályozó eszközök előírásai szerint.

e) Ha az elkövetett cselekmény kimeríti a Btk. valamely törvényi tényállását, akkor a vizsgálatért felelős személy köteles az elkövető felelősségre vonását kezdeményezni.

4. A felhasználó által jelentendő biztonsági esemény

A felhasználó köteles az általa észlelt informatikai biztonsági eseményről vagy annak bekövetkezési lehetőségéről értesíteni közvetlen vezetőjét.

A felhasználó köteles az informatikai biztonsági eseményt előidéző okokat megszüntetni, amennyiben erre saját hatáskörben vagy az eseményt előidéző személy bevonásával lehetősége van. Amennyiben ez nem lehetséges vagy nem járt sikerrel, a biztonsági esemény kezelésében köteles közreműködni, amennyiben erre a biztonsági esemény kezeléséért felelős személytől felkérést, utasítást kap.

A felhasználó a fentiek szerint köteles eljárni, amennyiben az alábbi körbe tartozó informatikai biztonsági eseményt észlel, vagy ilyenre gyanakszik:

a) a felhasználói azonosítóval való visszaélés, illetéktelen rendszer- vagy adathozzáférés, bármely, a felhasználó által használt szolgáltatás, rendszer, infokommunikációs eszköz tekintetében (pl. elektronikus levelezés, szakrendszer stb.),

b) adathalász tevékenység, amely a felhasználó személyes adatainak vagy intézményi hozzáféréseinek, illetve az intézményt érintő – nem publikus – információk megszerzésére irányul (pl. adathalász oldalak, kéretlen levelek vagy közvetlen telefonhívások, amelyek személyes vagy munkahelyi információk megszerzésére irányulnak),

c) rosszindulatú szoftverek (vírusok, trójai programok stb.) jelenléte a felhasználó által használt rendszeren, infokommunikációs eszközön,

d) adatszivárgás, ami megvalósulhat az érintett szervezet adatvagyonát képező nem közérdekű adatok szándékos vagy véletlen továbbításával, kiszivárogtatásával azok megismerésére nem jogosult szervezetek, személyek vagy az adatok bizalmasságának megőrzése szempontjából megbízhatatlan rendszerek felé,

e) felhasználó használatában lévő informatikai eszköz elvesztése, ezek megbontására utaló jelek.

5. Az informatikus munkakört ellátó munkatárs jogai és kötelezettségei

Az informatikus munkakört, szerepkört, feladatkört ellátó munkatárs a felhasználói jogosultságokon túlmutató többletjogosultságait csak a jogszabályokkal és a belső szabályzatokkal összhangban, rendeltetésszerűen, a munkaköri leírásában foglalt feladatok ellátásához használhatja.

A rendszergazda részletes felelősségét és hatáskörét a munkaköri leírása tartalmazza, amely magába foglalja az alábbiakat:

a) A HKK Hálózat biztonsági kockázatának minimalizálása.
b) Az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismerése és jelentése.
c) Az informatikai szabályok betartása és betartatása.

VIII. FEJEZET
ADMINISZTRATÍV BIZTONSÁGI KÖVETELMÉNYEK

1. Rendszerek dokumentálása

A rendszerek teljes életciklusát dokumentálni kell, így a tervezés (követelmény-meghatározás), a fejlesztés és a továbbfejlesztés vagy a beszerzés, a tesztelés és az ellenőrzés, az üzemeltetés, a fenntartás és a karbantartás, valamint a megszüntetés (kivonás, archiválás, megsemmisítés) fázisait is.

A dokumentáció teljességéért és naprakészségéért (folyamatos aktualizálásáért) a titkár, a rendszer üzemeltetésének megkezdésétől az üzemeltető felel.

A dokumentáció tartalmazza a rendszerben alkalmazott biztonsági megoldásokat, beleértve a rendszer egy esetleges részleges vagy teljes körű meghibásodása vagy megsemmisülése esetére kidolgozott eljárásrendet.

A rendszerek dokumentációjának őrzéséről, arra jogosultak számára hozzáférhetővé tételéről, továbbá folyamatos aktualizálásáról a klub titkára bevonásával az üzemeltetésért felelős személy gondoskodik.

IX. FEJEZET
ÜZLETMENET-FOLYTONOSSÁG ÉS SZOLGÁLTATÁS-FOLYTONOSSÁG BIZTOSÍTÁSA

1. Mentés és archiválás

A rendszerekben kezelt, feldolgozott, tárolt adatok rendelkezésre állását rendszeres és indokolt esetben soron kívüli mentéssel kell biztosítani.

Az érintett rendszerek esetében havonta egy rendszer szintű teljes mentést kell készíteni külső adattárolóra, amelynek elkülönített és biztonságos offsite tárolásáról kell gondoskodni. A teljes mentések elkülönített offsite tárolása féléves rotációval valósul meg.

A rendszerekben kezelt, feldolgozott, tárolt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során már nem szükséges, azonban őrzésük indokolt, archiválni kell.

A mentési és archiválási eljárásokat, a vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy azok

a) a szakmai bevált gyakorlatokon alapuljanak, kielégítő biztonságot adjanak az arányosság elvének figyelembe vételével,
b) a rendszereket érintő, jelentős meghibásodások és megsemmisülések hatásait hatékonyan kivédhetővé tegyék,
c) biztosítsák az adatvesztések elkerülését vagy minimalizálását.

X. FEJEZET
FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK

1. Kritikus adatokat tartalmazó számítógépek használata

Az adatvédelmi szempontból kritikus adatokat (különösen: személyügyi, pénzügyi információkat) tároló számítógépek védelmére fokozott figyelmet kell fordítani. Zárt, teljes körű, folytonos és kockázatokkal arányos, adatvédelmet és biztonságot kell biztosítani. Ezen gépek körét a klub elnöke határozza meg.

Mellékletek:

1. Az IBSZ karbantartása
2. Az adatvédelem, informatikai biztonság ellenőrzése
3. A személyes adatok tartalma és kezelői
4. Adatkezelési tájékoztató
5. Biztonsági események nyilvántartása