**A Bárka Kőbányai Humánszolgáltató Központ**

**IV/17-8/2024**

# Informatikai Biztonsági Szabályzata

Kiadta: Lehoczki Klára intézményvezető
Kiadás napja: 2024. 08. 01.

Lehoczki Klára Digitálisan aláírta: Lehoczki Klára
Dátum: 2024.07.12 12:06:06 +02'00'

Lehoczki Klára intézményvezető

Tartalom

I. A Bárka Kőbányai Humánszolgáltató Központ adatai ..... 3
Az intézmény adatai és elérhetőségei ..... 3
II. Általános rendelkezések ..... 3
A Szabályzat célja ..... 3
A Szabályzat hatálya és módosítása ..... 3
A Szabályzat Személyi, tárgyi és időbeli hatály: ..... 3
A Szabályzat módosítása ..... 3
Alapelvek ..... 4
Információbiztonsági kockázatfelmérés és –kezelés ..... 4
III. Az informatikai biztonság szervezete ..... 4
IV. Személyi biztonsági követelmények ..... 7
V. Informatikai biztonságot érintő események kezelése ..... 8
VI. A szolgáltatás-folytonosság biztosítása ..... 9
VII. Fizikai biztonsági követelmények ..... 10
Gépterem, szerverszoba kialakításával kapcsolatos szabályok ..... 10
Hozzáférés a rendszerekhez ..... 11
Az informatikai rendszerek használatának korlátai ..... 13
Internetelérés ..... 13
Elektronikus levelezés biztonsági szabályai ..... 14
Saját eszközök használatának biztonsági előírásai ..... 14
Szoftverjogtisztaság, szoftverek telepítése, frissítése ..... 15
Mobil adathordozók kezelése ..... 15
Kártékony kódok elleni védelem ..... 15
VIII. Záró rendelkezések ..... 16
IX. Mellékletek ..... 17
1. számú melléklet – Nyilatkozat az Informatikai biztonsági szabályzatának megismeréséről ..... 17

I. A Bárka Kőbányai Humánszolgáltató Központ adatai

Az intézmény adatai és elérhetőségei

| | |
|---|---|
| Név: | Bárka Kőbányai Humánszolgáltató Központ |
| Cím: | 1105 Budapest, Ihász utca 26. |
| Telefon: | +36 1 2618183 |
| Email: | barka@bkhk.hu |
| Weboldal: | www.bkhk.hu |

II. Általános rendelkezések

1. A Bárka Kőbányai Humánszolgáltató Központ (a továbbiakban: Intézmény) Informatikai Biztonsági Szabályzata (a továbbiakban: Szabályzat) az alábbiak szerint kerül megállapításra.

A Szabályzat célja

1. 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.

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

3. A Szabályzat aktualizálásáért az Intézmény informatikusa és az üzemeltetési csoport vezetője a felelős.

4. Jelen Szabályzat az informatikai biztonsági szabályozás alapdokumentuma, amely átfogóan és keretjelleggel szabályozza az információbiztonsági szempontból releváns kérdéseket.

A Szabályzat hatálya és módosítása

A Szabályzat Személyi, tárgyi és időbeli hatály:

1. A jelen Szabályzat személyi hatálya az Intézmény informatikai szolgáltatásait használó felhasználókra és rendszergazdára, tárgyi hatálya az Intézmény teljes infrastruktúrájára, azaz a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére, a folyamatokra, a székhelyre és valamennyi telephelyre és a létesítményekre is kiterjed a kiadás napjától kezdődően, annak visszavonásáig.

2. Jelen adatkezelési szabályzat hatályon kívül helyezi Bárka Kőbányai Humánszolgáltató Központ valamennyi korábbi Informatikai biztonsági szabályzatát, belső utasítását.

A Szabályzat módosítása

1. A szabályzat módosítására az intézmény bármely dolgozója javaslatot tehet az intézményvezetőnek megküldött, de az adatvédelmi tisztviselőnek címzett írásbeli megkeresésben.

2. A megkeresésnek tartalmaznia kell a dolgozó nevét, aláírását, elérhetőségét, a javasolt módosítást röviden összefoglalva, továbbá a módosítás szükségességét alátámasztó indokokat.

3. A megkeresés iktatás után kiszignálásra kerül az adatvédelmi tisztviselőhöz, aki megvizsgálja a javasolt módosításokat, elkészíti ajánlását a javasolt módosítás tekintetében.

4. A megkeresés az ajánlással együtt megküldésre kerül az üzemeltetési vezetőnek, illetve az intézményvezetőnek, aki jóváhagyja a módosítás előkészítését.

5. Az adatvédelmi tisztviselő és az üzemeltetési vezető előkészíti a módosítás tervezetét és megküldi az intézményvezetőnek egyeztetésre.

6. A módosítási eljárás szabályait a szakmai vezető, illetve intézményvezető megkeresése alapján indított módosítási eljárás esetében is megfelelően alkalmazni kell.

7. Az intézmény honlapján a módosítás előtti és utáni változatokat is közzé kell tenni a hatályba lépés és a hatályon kívül helyezés időpontjának megjelölése mellett.

8. A módosításokat az intézmény foglalkoztatottjaival, illetve folyamatban lévő ügyek esetében az érintettekkel meg kell ismertetni, amennyiben a változtatás érinti a folyamatban lévő adatkezelést.

Alapelvek

1. Az Intézmény Belső adatvédelmi és adatbiztonsági szabályzatának Adatbiztonságra vonatkozó fejezetében rögzített alapelvek (bizalmasság, rendelkezésre állás, sérthetetlenség) a jelen szabályzat alapját biztosítják, melyek további alapvetésekkel egészülnek ki.

2. 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.

3. 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.

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

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

Információbiztonsági kockázatfelmérés és –kezelés

Információbiztonsági kockázatfelmérés és –kezelés szabályait az Intézmény Belső adatvédelmi és adatbiztonsági szabályzata tartalmazza.

III. Az informatikai biztonság szervezete

1. Az intézmény valamennyi foglalkoztatottja számára kötelező az informatikai biztonsági szabályok és előírások betartása.

2. Az intézmény informatikai biztonsági szervezetének felépítése:
   a. intézményvezető
   b. üzemeltetési vezető
   c. informatikus

d. adatvédelmi tisztviselő
e. szervezeti egység vezető
f. felhasználó

1. Az intézmény vezetője
   a) gondoskodik az informatikai biztonság személyi és tárgyi feltételeinek biztosításáról,
   b) gondoskodik – szabályozás és ellenőrzés útján – az előírt, információbiztonsággal összefüggő tevékenységek végrehajtásáról,
   c) informatikai biztonsági kérdésekben dönt,
   d) Az elektronikus információs rendszerrel kapcsolatba kerülő munkatársak esetén elvégzi el a munkakörök, feladatok informatikai biztonsági szempontú besorolását és ezt évenként felülvizsgálja

2. Üzemeltetési vezető
   a) ellátja az Intézmény vonatkozásában az informatikai biztonsági szakmai irányítási és felügyeleti feladatokat, előkészíti a Szabályzatot, gondoskodik naprakészen tartásáról és oktatásáról,

3. Informatikus
   a) felelős az Intézmény informatikai tevékenységének jogszerűségért, beleértve az informatikai biztonsági tevékenységet,
   b) informatikai biztonsági fórumokon, az Intézmény nevében részt vesz,
   c) gondoskodik – az érintett szakterületek bevonásával – az információbiztonsággal összefüggő felsővezetői döntések előkészítéséről,
   d) közreműködik – az informatikai biztonsági szempontok meghatározásával – az informatikai biztonsággal összefüggő informatikai szakmai döntések előkészítésében,
   e) részt vesz a Belső adatvédelmi és adatbiztonsági szabályzatban rögzített adatbiztonsági ellenőrzésen
   f) részt vesz a biztonsági esemény kivizsgálásában
   g) felelős az Intézmény által üzemeltetett vagy fejlesztett rendszerek jogszerű és szakszerű működéséért, működtetéséért
   h) az intézményi munka informatikai támogatása, valamint azIntézmény Informatikai rendszereinek működtetése, továbbá a belső hálózati szolgáltatásokat, valamint az Intézmény internetes megjelenését, kapcsolattartását biztosító rendszerek folyamatos üzemeltetése;
   i) az informatikai rendszerek üzembiztosságának fenntartása, a hatályos szabályzatok, korlátozások betartásával elhelyezett adatok védelme;
   j) az informatikai rendszerek folyamatos karbantartása, fejlesztése, a lehetőségek mértékében a felmerülő igényekhez igazítása, az új technikai lehetőségek alkalmazhatóságának megteremtése;
   k) a rendszerbe állításra tervezett új informatikai és kommunikációs eszközök, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, előkészítő döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról, illetve az elavultak kivonásáról;
   l) 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;
   m) a felhasználók személyi számítógépeinek (asztali és hordozható gépek) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása, működési zavar, meghibásodás, rendellenes működésesetén a hibaelhárítás lehető leggyorsabb, de maximum 2 munkanapon belül

n) az informatikai rendszer és a szolgáltatások működéséhez, karbantartásához időközönként szükséges, előre tervezhető üzemszünetek, leállások 2 nappal a tervezett időpont előtt e-mailben történő bejelentése;
o) az általános informatikai ismereteken túli, az adott szolgáltatás igénybevételéhez szükséges ismeretek nyújtása.

4. Szervezeti egységvezető
   a) kezdeményezi az irányítása alá tartozó szervezeti egységek tevékenységével érintett rendszerekkel összefüggő informatikai szakmai és információbiztonsági intézkedéseket, beszerzéseket, illetve közreműködnek azok végrehajtásában,
   b) az informatikai biztonsággal összefüggő ellenőrzéseket tervez és hajt végre, illetve gondoskodik az ellenőrzések lefolytatásáról az adatvédelmi tisztviselővel és az informatikussal együttműködésben
   c) az informatikai biztonság megsértésének észlelése esetén azonnal jelenti azt az informatikusnak, az intézményvezetőnek, az adatvédelmi tisztviselőnek és javaslatot tesz az elektronikus információs rendszerek biztonságáért felelős személynek a megteendő intézkedésekre.
   d) a vezető jogosult és köteles az irányítása alá tartozó munkatársak munkavégzéséhez szükséges infokommunikációs eszközök, valamint a használandó rendszerek és azokhoz szükséges jogosultságok körét meghatározni, továbbá az előzőek biztosításához szükséges engedélyezési eljárásokat kezdeményezni, illetve lefolytatni.
   e) a vezető az informatikai biztonsági előírások megsértésnek észlelése esetén köteles: azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében, indokolt esetben kezdeményezni a rendszer használatának felfüggesztését, illetve üzemszüneti eljárásrend bevezetését, amennyiben meghatározható rendszerre korlátozódik a biztonsági előírások megsértése, kivizsgáltatni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására, a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni.

5. Adatvédelmi tisztviselő
   a) együttműködik az adatbiztonsági szabályok kialakításában
   b) közreműködik az adatbiztonsági ellenőrzés lefolytatásában
   c) amennyiben az Intézmény informatikai rendszerének fejlesztése, módosítása újabb informatikai alkalmazások fejlesztését, beszerzését indokolja, az adatvédelmi tisztviselő megvizsgálja, hogy az adatkezelés adatvédelmi szempontból a GDPR, illetve személyes adat kezelését előíró szabályzat hatálya alá esik-e, ennek eredményéről és az érintett személyes adatok köréről tájékoztatást ad az intézményvezető részére, hogy szükséges-e adatfeldolgozási szerződés megkötése

6) Felhasználó
   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 (az igény jogosságát a szakterület vezetőjével együttműködve az intézményvezető bírálja el).
   c) A felhasználó a rendelkezésére bocsátott infokommunikációs eszközöket csak az Intézmény céljaival, feladataival kapcsolatos, a munkaköri feladatai ellátásához szükséges tevékenység céljára, rendeltetésszerűen, a számára megállapított jogosultságok keretein belül, rendeltetésszerűen használhatja.

d) Az informatikai rendszerekhez vagy eszközökhöz bármilyen berendezést (különösen: számítógépeket, perifériákat – nyomtató, scanner külső adattárolók – fax, okostelefon, stb.) csak az informatikus 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 egyetemi 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 számítástechnikai eszközöket munkavégzésen kívüli célra nem használhatja.
m) A felhasználó köteles a saját feladatkörében nem megoldható informatikai biztonsági problémáról, hiányosságról értesíteni közvetlen vezetőjét és az adatvédelmi tisztviselőt és közreműködni a szükséges intézkedések végrehajtásában.
n) A felhasználó köteles meghibásodás, üzemzavar észlelésekor, vírusfertőzés (vagy annak gyanúja) esetén haladéktalanul értesíteni az informatikust, a számítógép további használatát az informatikus intézkedéséig felfüggeszteni. A hibaelhárítás folyamán az informatikussal együttműködni, számára a szükséges információkat megadni.

IV. Személyi biztonsági követelmények

1) Az elektronikus információs rendszerrel kapcsolatba kerülő munkatársak esetén el kell végezni a munkakörök, feladatok informatikai biztonsági szempontú besorolását és ezt évenként felül kell vizsgálni.
2) Az egyes az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt a jogosultság jóváhagyója köteles ellenőrzi, hogy az érintett személy a besorolásnak megfelelő feltételekkel rendelkezik-e.
3) Minden munkatárs köteles a részére átadott informatikai eszközt, vagyontárgyat az Intézmény részére visszaszolgáltatni a jogviszonyának megszűnése előtt.

4) 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, amennyiben annak feltételei adottak. Külön figyelmet kell fordítani és messzemenően be kell tartani az információk/adatok minősítésére vonatkozó előírásokat.

5) A nyomtatókról azonnal el kell távolítani a kinyomtatott iratokat.

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

7) Az új belépő munkatársat, a munkába állásának kezdetekor, de 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 az Intézmény 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. Az informatikai biztonsághoz kapcsolódó oktatás az évenkénti adatvédelmi oktatással összekapcsolható.

## V. Informatikai biztonságot érintő események kezelése

1) Biztonsági esemény az a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változás 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.

2) 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.

3) Az a foglalkoztatott, aki az intézmény által működtetett informatikai rendszerhez kapcsolódó biztonsági eseményt észlel, azt köteles a közvetlen vezetője értesítése mellett 60 percen belül az informatikusnak bejelenteni, megadva a nevét, a biztonsági esemény tárgyát, valamint azt, hogy a biztonsági esemény személyes adatokat érint-e. A bejelentő további olyan információkat is megadhat, amelyeket biztonsági esemény beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

4) Biztonsági eseményre utalhat, melyet a felhasználóknak azonnal jelenteniük kell, ha
   a) szolgáltatás, a berendezés vagy az eszközök elvesztése történik,
   b) rendszer rendellenes működését észlelik,
   c) a szabályzatoknak vagy irányelveknek való nem-megfelelés válik nyilvánvalóvá,
   d) észlelhető a fizikai biztonsági rendelkezések megsértése,
   e) nem ellenőrzött rendszerbeli változásokat tapasztalnak,
   f) a szoftver vagy hardver hibás működése lép fel,
   g) jogosulatlan hozzáférést tapasztalnak.

5) Amennyiben a biztonsági esemény személyes adatokat is érintően következett be, akkor az észlelő tájékoztatja az adatvédelmi tisztviselőt.

6) Az informatikus személyes adatokat is érintő biztonsági esemény esetén az adatvédelmi tisztviselővel együttműködve – a bejelentést megvizsgálja, a bejelentőtől adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb 2 munkanapon belül teljesíteni.

7) Az adatszolgáltatásnak tartalmaznia kell
   a) a biztonsági esemény bekövetkezésének időpontját és helyét
   b) a biztonsági esemény leírását, körülményeit, hatásait
   c) a biztonsági esemény során kompromittálódott adatok körét, számosságát,
   d) a kompromittálódott adatokkal érintett személyek körét
   e) a biztonsági esemény elhárítása érdekében tett intézkedések leírását,
   f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását

8) Az informatikus és személyes adatokat érintő biztonsági esemény esetén az adatvédelmi tisztviselő javaslatai alapján az intézményvezető a biztonsági esemény jellegétől függő intézkedéseket megteszi a biztonsági esemény és az adatvédelmi incidens negatív következményeinek elhárítása és a hasonló incidensek megelőzése érdekében.

## VI. A szolgáltatás-folytonosság biztosítása

1) Az elektronikus információs rendszer folyamatos működését biztosítani kell.

2) A folyamatos működés biztosítása érdekében az Intézmény által üzemeltetett rendszerek esetében infrastruktúra szinten két, azonos funkcionalitású adatközpont kialakításról kell gondoskodni. A két csomópontos kialakítást földrajzilag különböző elhelyezkedésű objektumokban kell megvalósítani (ezt nevezik geo-redundáns elhelyezésnek). Ennek célja a helyi infrastrukturális hibáknak (pl.: áramszünet stb.) és vis major eseményeknek (villámcsapás, tűz, árvíz, stb.) az informatikai szolgáltatás minőségére és biztonságára gyakorolt hatásainak csökkentése.

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

4) Az Intézmény működése során használt rendszerek esetében naponta egy automatikus mentést kell végrehajtani. A kritikus rendszerekről a mentés eredményét az adott rendszer tárolja, a két site-os rendszerekben a mentés eredményét a túloldali site-ra is replikálni kell.

5) Az érintett rendszerek esetében legalább hetente egy, rendszerszintű teljes mentést kell készíteni, amelynek elkülönített és biztonságos off-site tárolásáról az informatikus gondoskodik. A teljes mentések elkülönített off-site megőrzéséről legfeljebb 30 napig kell gondoskodni, melynél hosszabb időt egyetemi szabályzat megállapíthat. Eltérő rendelkezés hiányában a 30. nap elteltét követően a teljesmentéseket a mentőrendszer automatikusan törli.

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

7) Az adatállományt – amennyiben személyes adatot is tartalmaz – az őrzési idő elteltével törölni kell.

8) 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.

9) A mentési tervet az informatikus alakítja ki a jogszabályi, belső-, és külső előírások, valamint a technológiai lehetőségek figyelembe vételével.

10) A rendszerekben kezelt, a felhasználók számára a munkavégzéshez már nem szükséges adatállományokat törölni kell. A törlés megtörténtéről jegyzőkönyvet kell felvenni.

VII. Fizikai biztonsági követelmények

1) Az Intézmény informatikai rendszere tűzfalakkal védett.

2) Az adatvédelmi szempontból kritikus adatokat (különösen: személyügyi, pénzügyi, ügyviteli adatokat, információkat, kliensek adatait) tároló számítógépek védelmére fokozott figyelmet kell fordítani.

3) Az rendszereket, rendszerelemeket, infokommunikációs eszközöket úgy kell telepíteni és tárolni, hogy
   a. a lehető legkisebb mértékre csökkentsék a fizikai és környezeti veszélyekből adódó lehetséges károkat,
   b. azokhoz a jogosult munkatársakon és az Egyetemmel polgári jogi jogviszonyban álló személyeken kívül más személy hozzáférése – jogosulatlan hozzáférés – kizárt (a lehető legkisebb mértékűre csökkentett) legyen.

4) A környezeti feltételeket a befogadó helyiségek rendeltetése, a telepítési környezetek alapján az alábbiak szerint kell meghatározni:
   a) irodai környezet (jellemzően a felhasználói és az általános informatikai tevékenységet támogató munkaállomások befogadására szolgáló helyiségek),
   b) kiemelt informatikai munkaterület (speciális, az irodai környezet védelmi igényét meghaladó informatikai eszközök befogadására szolgáló helyiségek, pl. fejlesztői körlet, informatikai eszközök raktára stb.),
   c) gépterem (az informatikai erőforrásokat koncentráltan tartalmazó helyiségek, pl. a rendszerek, szolgáltatások központi üzemeltetését és irányítását végző infokommunikációs eszközöket befogadó létesítmények, csomópontok, adatközpontok, számítóközpontok, szerverszobák, kommunikációs elosztóhelyiségek stb.).

5) Az informatikai rendszerbe tartozó aktív eszközök feszültségmentesítését (kikapcsolását) áramszünet, természeti csapás (különösen: tűz, vízbetörés vagy más rendkívüli esemény), áramütés, vagy annak gyanúja, egyértelmű készülék meghibásodás (különösen: füst, látható zárlat vagy más látható műszaki hiba) kivételével csak arra kioktatott személyek végezhetik.

Gépterem, szerverszoba kialakításával kapcsolatos szabályok

a) belépés és beléptetés rendje,
b) fizikai behatolás-riasztások és felügyeleti berendezések kezelése,
c) áramellátás, rövid távú, szünetmentes és hosszú távú, tartalék áramellátás,továbbá kábelezés megvalósítási módja,
d) vészhelyzeti kikapcsolás megvalósítási módja,
e) automatikus vészvilágítási rendszer alkalmazása és karbantartása,
f) tűzvédelem,
g) hőmérséklet- és páratartalom biztosítása,
h) csővezeték-rongálódásból származó károkkal szembeni védelem,
i) a helyiségben végzendő javító, karbantartó, takarító stb. tevékenységek végzésének rendje

Hozzáférés a rendszerekhez

1) A felhasználó a rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.

2) A rendszer használata során a felhasználó egyedi azonosítását folyamatosan biztosítani kell. Minden felhasználót kizárólagos személyi használatú azonosítóval kell ellátni, amelyhez egyedi jelszót kell rendelni.

3) A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:
   a) Tilos a felhasználóra jellemző, könnyen kitalálható (különösen: vezetéknév, keresztnév, saját gyermekek, ismert kedvenc személy, kedvenc háziállatok, stb.) jelszavakat választani.
   b) Tilos a login nevet jelszóként használni.
   c) Tilos azonos vagy az abc-ben, a billentyűzeten egymást követő számokból vagy betűkből álló jelszót használni.
   d) A jelszó hossza nem lehet rövidebb nyolc karakternél, de 20 karakter maximumú lehet), tartalmaznia kell legalább kettő (maximum 18) számjegyet, valamint legalább egy nagybetűt, és minimum egy (maximum 17) kisbetűt. A jelszó ékezetes betűt nem tartalmazhat. Jelszavak választásakor javasolt a számok, a kis- és nagybetűk keverése, a könnyebb megjegyezhetőség érdekében rövid jelmondatok szóköz nélküli, és a szavak nem szótári alakban történő használata stb.
   e) Tilos a jelszót nyilvános helyen kiírva tartani (különösen: monitorra ragasztva).
   f) A hálózati belépésre jogosító jelszót kötelező – az egyéb jelszavakat ajánlott rendszeresen, de legalább – 180 naponta újra cserélni.

4) A felhasználók a Hálózathoz, rendszerekhez történő hozzáférést biztosító jelszavakat – első alkalommal – az illetékes rendszergazdáktól lezárt borítékban kapják meg, vagy a felügyeletükben a felhasználók saját maguknak állítják be. A borítékban kiadott jelszavakat az első belépést követően azonnal módosítani kell.

5) Az elfelejtett, lejárt jelszavak helyett új jelszavak kiadása csak személyesen, az illetékes rendszergazdánál az első alkalommal történt jelszavak kiadásához hasonlóan történik.

6) Az Intézmény informatikai rendszeréhez történő hozzáférés – jelszóigénylés – jogosultságának ellenőrzése érdekében az informatikus kérheti a felhasználó érvényes „személyazonosításra alkalmas hatósági igazolványát" (személyazonosító igazolványát, vagy útlevelét, vagy kártyaformátumú vezetői engedélyét).

7) A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelen személy általi megismerését kizárni. Amennyiben a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett (biztonsági esemény), abban az esetben a biztonsági esemény fejezetnél meghatározott szabályok szerint kell eljárni.

8) A szakmai vezetők javaslatai alapján az informatikus lehetővé teszi a kijelölt felhasználók részére az intézményi informatikai rendszer bizonyos részeinek távoli elérését. A távoli munkavégzés során is be kell tartani a biztonsági rendszabályokat, különös tekintettel az illetéktelen hozzáférés megakadályozására. A távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó titkosított formában haladjon, valamint az adatforgalmat is titkosítani kell.
   A távoli munkavégzés során VPN segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme, az illetéktelen hozzáférés megakadályozása a felhasználó kötelessége és felelőssége.

9) A felhasználó részére csak a munkaköre ellátásához szükséges és elégséges jogosultságok adhatók ki. A rendelkezés megtartásáért a felhasználó közvetlen vezetője a felelős. A jogosultságokat úgy kell kialakítani, hogy megkülönböztethetők legyenek a felhasználói és a privilegizált felhasználói jogosultságok, jogosultságcsoportok. A jogosultságokat felhasználói csoportokhoz kell rendelni; a munkatársak felhasználói csoportbeli tagsága biztosítja a jogosultságok használatát. A felhasználó a számára engedélyezett szolgáltatásokat, alkalmazásokat, szoftvereket mások számára semmilyen módon nem teheti hozzáférhetővé, illetve az infokommunikációs eszközöket nem használhatja más felhasználó nevében (indokolt esetben betekintési jogot adhat az általa kezelt adatokba, pl. postafiókjába). A felhasználó helyettesítése esetén a helyettes bejelentkezése saját néven, saját – szükség esetén határozott időtartamra igényelt külön – jogosultsággal történhet.

10) Amennyiben a felhasználó jogviszonya megszűnik, továbbá ha a jogviszonyában olyan változás következik be, amely miatt a munkavégzéséhez a korábban igényelt jogosultságok nem szükségesek, amennyiben a jogosultságok visszavonása nem történik meg informatikai rendszer által támogatottan automatikusan, a felhasználó közvetlen vezetője köteles a jogosultságok visszavonását kezdeményezni.

11) A jogosultságot a felhasználó számára az intézményvezető engedélyezheti vagy vonhatja vissza. A jogosultság csak ezt követően állítható be.

12) Jogosultsági szint összefoglaló táblázat

| Szint | Jogosultak | Jogok | Felelős |
|---|---|---|---|
| Külsős | Intézményi vendégek, kliensek, látogatók | Internet elérés, vendég WiFi használat | Szakmai vezető |
| Alap | Intézmény dolgozói | Internet elérés, WiFi használat<br>Egyéni azonosítás alapján lehetővé válik a munkához szükséges adatok, programok, levelezés, | Szakmai vezető |
| Adminisztrátor | Adminisztrációval kapcsolatos munkakörök | Internet elérés, WiFi használat<br>Alapszint+hozzáférés az adminisztrációs, dokumentációs rendszerekhez, szervezeti egység közös lemezterületéhez | Szakmai vezető |
| Gazdasági | gazdasági ügyintéző | Internet elérés, WiFi használat<br>Alapszint+hozzáférés a gazdálkodással és a dolgozókkal kapcsolatos rendszerekhez | Intézményvezető |
| Humánpolitikai | munkaügyi ügyintéző | Internet elérés, WiFi használat<br>Alapszint+hozzáférés a dolgozókkal | Intézményvezető |

| | | | |
|---|---|---|---|
| | | kapcsolatos rendszerekhez. | |
| Rendszergazda | informatikus, üzemeltetési vezető intézményvezető | Korlátlan jog a rendszergazda által felügyelt rendszerekhez (különösen: hálózat, storage, szerverek, adatbázisok, mentési rendszer, egyetemi szervezet által felügyelt szerver) | Intézményvezető |

Az informatikai rendszerek használatának korlátai

Az Intézmény informatikai rendszereit tilos használni az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

a) A mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, mások személyiségi jogainak megsértése (különösen: rágalmazás, stb.), tiltott haszonszerzésre irányuló tevékenység (különösen: piramisjáték, stb.), szerzői jogok megsértése (különösen: szoftver és médiatartalom nem jogszerű megszerzése, tárolása, terjesztése).
b) Másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf, pedofil anyagok közzététele).
c) A hálózati erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás/szolgáltatás eredeti céljától idegen (különösen: hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenetküldése).
d) Mások munkájának zavarása vagy akadályozása (különösen: kéretlen levelek,hirdetések).
e) A hálózati erőforrások magán célra való túlzott mértékű használata.
f) A hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (különösen: elektronikus levélbombák, hálózati játékok, kéretlen reklámok, online fájlmegosztás, digitális fizetőeszköz bányászat, stb.).
g) A Hálózat erőforrásaihoz, a Hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – illetéktelen szisztematikus próbálgatása (különösen: TCP/UDP port scan).
h) Hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (un. spoofing).
i) A Hálózat bármely szolgáltatásának szándékos, vagy hiányos ismeretekből, nem megfelelő körültekintéssel végzett beavatkozásokból fakadó zavarása, illetve részleges vagy teljes bénítása (leszámítva a rendeltetésszerű használat fenntartásához szükséges, a hálózati rendszergazdák, rendszermérnökök általi tudatos beavatkozásokat).

Internetelérés

1) Az Intézmény eszközein biztosított internetelérés a munkavégzést, az intézményi célokat hivatott szolgálni, éppen ezért elsősorban az Intézményi munkavégzéssel kapcsolatos feladatok felelősségteljes végzése támogatott.

2) A munkaállomások alaphelyzetben (a speciális rendeltetésű számítógépek kivételével) rendelkeznek internet eléréssel. Az Intézmény fenntartja a jogot arra, hogy a vonatkozó törvények betartásával, és az azoktól kapott felhatalmazás alapján – különös tekintettel a Büntető Törvénykönyvben és az elektronikus hírközlésről szóló 2003. évi C. törvényben

foglaltakra – az intézményi informatikai rendszerek használata folyamán (a rendszer biztonságos, és rendeltetés szerinti használatának, optimális leterheltségének, sebességének kialakítása, fenntartása érdekében) a felhasználók internetforgalmát, tartalmát figyelemmel kísérje és naplózza, a veszélyes internetes honlapok elérését letiltsa.

Elektronikus levelezés biztonsági szabályai

1) Az e-mail címek lehetnek személyhez, szervezethez vagy egyéb csoporthoz (pl. projekt) rendelve. Az Intézmény informatikai rendszerén biztosított levelezés a munkavégzést, az intézményi célokat hivatott szolgálni, éppen ezért elsősorban az Intézményben történő munkaköri feladatokkal kapcsolatos feladatok felelősségteljes végzése támogatott. Intézményi e-mail cím kizárólag munkavégzéssel összefüggésben használható.
2) Az előző pontban leírt célok elérése érdekében és szükség esetén – különösen biztonsági okokból – a Hálózat terheltségének csökkentése érdekében a külső levelező rendszerek elérése tiltásra kerülhet.

3) A szükséges e-mail címeket az informatikustól lehet igényelni. Az igénylés előterjesztésével a felhasználó elismeri jelen Szabályzat ismeretét és vállalja az abban foglaltak betartását.

4) A jogviszony megszűnése után az intézményi postafiók (levelezési cím) adattartalmát az informatikus lementi és azt 5 évig megőrzi.

5) A felhasználó által a használt postafiókok esetében a postaládában szabályzatellenesen tárolt adatok az Intézmény Belső adatvédelmi és adatbiztonsági szabályzatában megjelöltek szerinti időpontban és módon kerülnek törlésre, amennyiben azok személyes adatokat tartalmaznak.

6) A megszűnés után az e-mail címet az informatikus 6 hónapig új belépő számára nem adja ki újra, ezen időtartamot követően az e-mail cím szabadon felhasználható.

7) Az Intézmény működésével kapcsolatos levelezéshez, kiadványokban történő megjelentetéshez csak a hivatalos intézményi e-mail címek használhatók.

Saját eszközök használatának biztonsági előírásai

1) A saját eszköz használatát a munkavégzéshez az intézményvezető engedélyezheti az alábbi feltételekkel:
    a. A saját eszközön tárolt munkahelyi adatok biztonságáért az eszköz tulajdonosa teljes körű felelősséggel tartozik.
    b. A saját eszközön az operációs rendszer, biztonsági csomag, irodai rendszerek utolsó biztonságos frissítése használható, ezért javasolt aktivizálni ezek automatikus frissítés funkcióját. (A biztonsági frissítéseket a programgyártók ingyenesen teszik elérhetővé.)
    c. Saját eszközön bizalmas és minősített adatok, valamint személyes adatok tárolása tilos, azokon csak nyilvános adatok tárolása engedélyezett!
    d. Az eszközt számítástechnikai hálózathoz, internethez csatlakoztatni csak biztonságos körülmények között szabad. A vezeték nélküli- WiFi-, bluetooth- kapcsolat csak biztonságos körülmények között használható, ezután kikapcsolásuk ajánlott (nyilvános helyeken – különösen szórakozóhelyek, üzletek, állomások területén elérhető hálózatok használata nem ajánlott).
    e. A saját eszközön tárolt adatok (különösen: WiFi illetve bluetooth kapcsolaton keresztül) akár a tulajdonos, a használó tudtán kívül is lemásolhatók. Amennyiben a biztonsági esemény (különösen: az intézményi adatok illetéktelen másolása, vagy a hitelessége, bizalmassága, sértetlensége egyéb módon sérül, stb.) az eszköz tulajdonosának gondatlanságából vagy neki felróható módon (különösen: program frissítések kikapcsolása, az eszköz gondatlan tárolása, szállítása, stb.) következik be, az így okozott károkért teljes körű felelősséggel tartozik.

f. A saját eszközön történő intézményi feladatokkal kapcsolatos munkavégzéshez szükséges adatokat külön könyvtárban (könyvtárrendszerben) kell tárolni, amely kialakításához – kérés, szükség esetén – az informatikus segítséget nyújt, illetve az eszközt érintő biztonsági esemény esetén az informatikus részére hozzáférést kell biztosítani. Egyúttal ki kell jelölni az intézményi hálózatra történő mentések helyét.
g. A munkahelyi célokra létrehozott könyvtárak intézményi rendszerre történő rendszeres mentésére fokozott figyelmet kell fordítani. A mentés a felhasználó kötelessége.
h. A jogviszony és a hozzáférési engedély megszüntetése után az intézményi munkavégzéssel kapcsolatos adatokat, és az intézményi licencek alapján telepített programokat az eszközről visszaállíthatatlanul törölni kell, amit végezhet az intézmény illetékes szakembere, vagy az eszköz tulajdonosa, használója. A visszaállíthatatlan törlést végző személy írásos nyilatkozatot tesz a végrehajtásról.

Szoftverjogtisztaság, szoftverek telepítése, frissítése

1) A számítógépekre csak jogtiszta szoftverek telepíthető.

2) A telepítéseket, frissítéseket az informatikus végzi.

Mobil adathordozók kezelése

1) Az Intézmény vagyonkezelésében levő mobil adathordozók kizárólag munkavégzéssel összefüggő célokra használhatók. Alkalmazásuk abban az esetben engedélyezett, ha a gazda eszköz (számítógép, tablet stb.) menedzselt eszköz és képes a csatlakoztatott mobil adathordozón kártékonykód-ellenőrzést végezni.

2) A mobil adathordozókat a rajtuk tárolt vagy tárolandó adatok védelmi előírásainak megfelelően kell kezelni. Különleges adat tárolása esetén legalább jelszavas védelem szükséges a rajtuk tárolt adatokhoz való hozzáféréshez, melyről a felhasználónak kell gondoskodnia.

3) A mobil adathordozók azonosítását nyilvántartási szám feltüntetésével (címkézés), mozgásuk nyomon követhetőségét az átadás-átvétel, továbbítás, selejtezés, megsemmisítés dokumentálásával biztosítani kell. Amennyiben a címkézés nem kivitelezhető, egyedi módon szükséges gondoskodni az azonosításról (pl. kísérő lap a gyárilag beépített adathordozók esetében).

4) Mobil adathordozó szállítása során a szükséges védelmi intézkedés megtételéért a felhasználó felelős.
5) A mobil adathordozók esetében alkalmazandó adatmentesítési eljárás az üzemeltetési alapeljárásban történő adattörlés.

6) Az üzemeltetési alapeljárásban történő adattörlést (formattálás, image készítése) az adathordozó újbóli használatra alkalmassá tétele érdekében helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal az informatikus napi tevékenysége során hajtja végre a vonatkozó folyamatleírásban foglalt szabályok szerint.

Kártékony kódok elleni védelem

1) A kártékony kódok elleni védelmi eljárásokat, a vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy azok az elektronikus információs rendszert annak belépési és kilépési pontjain védjék a kártékony kódok ellen, felderítsék és megsemmisítsék azokat, valamint:
   a. a folyamatos felügyelet ellátását lehetővé tegyék,
   b. támogassák a valós riasztások kiszűrését,
   c. alkalmasak legyenek a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,

d. tegyék lehetővé a kártékony kódok elleni védelem általános helyzetének értékelését,
e. biztosítsák az új fenyegetések időben történő felismerését, frissítsék a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg,
f. tegyék lehetővé a riasztások és a védelmi rendszer állapotában bekövetkező változások naplóelemző rendszerbe történő továbbítását

2) A számítógép számítógépes vírussal vagy más rosszindulatú programmal, történő fertőződése súlyos biztonsági kockázat. Az Intézmény informatikai rendszerében az informatikus által központilag biztosított, felügyelt többszintű vírusvédelmi rendszer működik. Ha ennek ellenére valamelyik számítógép, felhasználói munkaállomás vírussal fertőződik, az informatikus – a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében – kizárhatja azt a hálózati forgalomból.

3) A kártékony kódok elleni védelmi mechanizmusokat frissíteni kell minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg. A frissítéseket a konfigurációkezelés szabályaival és eljárásaival összhangban kell elvégezni.

## VIII. Záró rendelkezések

1) Az Informatikai Biztonsági Szabályzat 2024. 08. 01. napon lép hatályba.

2) A jelen szabályzat hatályának fenntartásáról az intézményvezető köteles gondoskodni. A IV/20-12/2020. iktatószámú Informatikai biztonsági szabályzat a mai nappal hatályon kívül helyezve.

3) A szabályzatot az Intézmény minden foglalkoztatottjával meg kell ismertetni, illetve hozzáférhetővé kell tenni számukra:
   a. Az Intézmény honlapján elektronikus formában elérhető minden munkatárs számára.
   b. Az intézményvezető irodájában, valamint minden szervezeti egységnél egy-egy nyomtatott példány megtalálható, ahol az Intézmény foglalkoztatottjai megtekinthetik azt.
   c. a munkaköri leírásban a feladatokat fel kell tüntetni.

IX. Mellékletek

1. számú melléklet – Nyilatkozat az Informatikai biztonsági szabályzatának megismeréséről

**Jelen nyilatkozat aláírásával kijelentem, hogy a Bárka Kőbányai Humánszolgáltató Központ Informatikai biztonsági szabályzatát a mai napon megismertem:**

| Sorszám | Név | Beosztás | Megismerés dátuma | Aláírás |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |