Szombathelyi Egészségügyi és Kulturális Intézmények
Gazdasági Ellátó Szervezete
9700 Szombathely, Wesselényi M. u. 4.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2024. január 1.

Szabályzat neve: Informatikai Biztonsági Szabályzat	**Iktatószáma:** **Sz/40-1/2024.**	**Oldalszáma:** **12 oldal** **+ 6 melléklet**

Készítette	Porpáczy István műszaki csoportvezető
Ellenőrizte	Kovács Andrea általános igazgatóhelyettes
Jóváhagyta	Vigné Horváth Ilona igazgató

Eredeti 1 példány készült.

Eredeti példány fellelhető: Általános igazgatóhelyettes irodája

A hatályos elektronikus változat (pdf formátumban) a dolgozók számára az intézmény belső hálózatán elérhető Szabályzatok mappában található.

Mit módosított: 2017. október 1. napjától hatályos szabályzatot

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A Szombathelyi Egészségügyi és Kulturális Intézmények Gazdasági Ellátó Szervezete Informatikai Biztonsági Szabályzatát (továbbiakban: IBSZ) a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat alapvető célja, hogy az **informatikai rendszer alkalmazása során is** biztosítsa az intézménynél az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya az intézmény valamennyi munkavállalójára, továbbá az informatikai eljárásban résztvevő más szervezetek munkatársaira egyaránt kiterjed.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- kiterjed az informatikai folyamatban szereplő összes fejlesztési, szervezési, programozási, üzemeltetési dokumentációra
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Az adatkezelés során használt fontosabb fogalmak

1. *Személyes adat:* bármely meghatározott (azonosított, vagy azonosítható) természetes személlyel (érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül, vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

2. *Különleges adat:*

   a.) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra,

   b.) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat.

3. *Adatkezelés:* az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így például azok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személyes azonosításra alkalmas fizikai jellemzők rögzítése is.

4. *Adattovábbítása:* ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik.

5. *Nyilvánosságra hozatal:* ha az adatot bárki számára hozzáférhetővé teszik.

6. *Adatfeldolgozás:* az adatkezelési művelethez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

7. *Személyes adat – nyilvántartó rendszer:* személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető.

8. *Adatállomány:* konkrét nyilvántartó rendszerben kezelt adatok összessége.

9. *Ügymenet kiszervezése:* Adatkezelő tevékenysége valamely részének végzésére mást bíz meg.

10. *Adatmegsemmisítés:* az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése.

11. *Adatvédelmi incidens:* személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

12. *Egészségügyi dokumentáció:* a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától.

13. *Adatbiztonság:* Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

14. *Rendszergazda*: az intézménynél a műszaki, informatikai csoportvezető munkakört betöltő munkatárs

4. Kapcsolódó szabályozások

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:
- Szervezeti és Működési Szabályzat
- Iratkezelési Szabályzat
- Adatvédelmi és incidenskezelési szabályzat
- Közérdekű adatok közzétételi szabályzat
- Közérdekű adatok megismerésének rendje
- Kommunikációs Szabályzat

5. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:
- a környezeti infrastruktúra
- a hardver elemek
- az adathordozók
- a dokumentumok
- a szoftver elemek
- az adatok
- a rendszerelemekkel kapcsolatba kerülő személyek

5.1. A védelem tárgya

A védelmi intézkedések kiterjednek:
- a rendszer elemeinek elhelyezésére szolgáló helyiségekre
- az alkalmazott hardver eszközökre és azok működési biztonságára
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára
- a személyhez fűződő és vagyoni jogokra

5.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi

intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

6. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére biztosítani kell.

6.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

6.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok
- minősített, titkos adatok

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. (1. sz. melléklet)

A titkot képező adatok védelmét, a feldolgozás - az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal az adott lehetőségekhez mérten is biztosítani kell (szoftver, hardver adatvédelem).

7. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

7.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
  - földrengés
  - árvíz

- tűz
- villámcsapás stb.

- Környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának felszökése vagy leesése,
  - piszkolódás (pl. por).

- Közüzemi szolgáltatásba bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

7.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:
- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:
- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a jelszó gyakori megváltoztatásának az elmulasztása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

8. A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

9.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos
  - betartása

9.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése
- helytelen adatkezelés
- programtesztelés elhagyása

9.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság
- szervezetlenség
- képzetlenség
- szándékosan elkövetett illetéktelen beavatkozás
- illetéktelen hozzáférés
- üzemeltetési dokumentáció hiánya

10. Az informatikai eszközök környezetének védelme

10.1. Vagyonvédelmi előírások

- a számítógéppel ellátott irodák külső és belső helyiségeit zárakkal kell felszerelni,
- csak az illetékes dolgozók tartózkodhatnak a számítógéppel ellátott irodákban,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a számítógéppel ellátott irodákba történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működtetéséért a felhasználó felelős.
- a központi tárolók és szerverek tárolására alkalmas helyisége(ke)t távfelügyeletre kötött vagyonvédelmi riasztórendszerrel kell ellátni.

10.2. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni.
- használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és visszahelyezni
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

10.3. Tűzvédelem

A számítógéppel ellátott irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

11.1. Az számítógéppel ellátott irodák védelme

Elemi csapás *(vagy más ok)* esetén a számítógéppel ellátott irodákban bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

11.2. Az eszközökkel szembeni vagyoni felelősség

A személyre kiadott, leltáron szereplő informatikai eszközökért, telefonokért a felhasználó vagyoni felelőséggel tartozik. A nem rendeltetés szerű használatból adódó károkat köteles megtéríteni. Az eszközök hiánya esetén jegyzőkönyvben rögzíteni kell az eseményt és a felelősség tényét.

11.3. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,

- a tapasztalatokat,

- a hardver tesztek által feltárt hibákat.

Alapgép szétbontását (kivéve a garanciális gépeket) csak a rendszergazda végezheti el.

11.4. Az informatikai feldolgozás folyamatának védelme

11.4.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses és optikai adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftver védelme. A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.

11.4.2. Hozzáférési lehetőség

A szerver(ek) rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát zárható szekrényben kell tárolni, a módosításokról nyilvántartást vezetni.

11.4.3. Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, filekezelő rutinok alkalmazásával lehet biztosítani.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

11.5. Selejtezés, sokszorosítás, másolás

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan, CD-t, pendrive-t, külső HDD-t ha a kapacitás a névleges érték 90 %-ánál kevesebb,
- véglegesen elhasználódott anyagot

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

11.6. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A mentést meghatározott időszakonként el kell végezni (napi-heti-havi-éves).

A munkák során a helyi gépeken, munkaállomásokon létrehozott és tárolt dokumentumok mentése az azt létrehozó munkatársak *(felhasználók)* feladata, illetve azt az adott program kezelésével megbízott dolgozó végzi el a központi hálózati tárolóegységre.

A központi tárolóegységen tárolt adatokról offline mentés készül a rendszergazda által meghatározott időszakonként, melynek tárolását más helyiségben, lehetőleg eltérő tűzszakaszban kell biztosítani.

A számítógépeken csak az engedélyezett és érvényes licenszekkel rendelkező alkalmazásokat, programrendszereket lehet telepíteni, futtatni, melyeket az 5. sz. melléklet tartalmazza. Egyéb szoftverek telepítése tilos! Amennyiben indoklás alapján szükségessé vált egyéb alkalmazás telepítése, azt a vezető kezdeményezésére a rendszergazda telepítheti és azt a nyilvántartásba felveszi. Ha egy alkalmazás szükségtelenné vált, akkor annak mentését el kell végezni és törölni az adott eszközről, majd a nyilvántartásban rögzíteni a használat végét.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adathordozókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

11.7. Szoftver védelem

11.7.1. Rendszerszoftver védelem

A rendszerszoftvereket naprakész állapotban kell tartani, ami az automatikus frissítési szolgáltatás beállításával érhető el. Az automatikusan nem frissülő programokat időszakosan a rendszergazda ellenőrzi és szükség esetén frissíti.

Teendők a következők:

- az üzembiztonság érdekében operációs rendszer biztonsági másolatával kell rendelkezni, amely szükség esetén azonnal betölthető legyen,

- a rendszerszoftverben módosításokat csak a rendszergazda végezhet. Ezekről a dokumentációkban is a változásokat át kell vezetni.

11.7.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem.
A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A programokról naprakész nyilvántartást kell vezetni, amelynek. legalább az alábbi adatokat kell tartalmaznia:
- a program verziószáma,
- a program készítőjének neve,
- a használatbavétel kezdete,
- a program megnevezése.

A program dokumentáció a rendszerdokumentációnak része.

11.8. Programok megőrzése, nyilvántartása

- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

11.9. Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten kell tárolni a telepítőkészleteket és a meghatározott rendszerességű mentéseket.

11.10. Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezettségű dokumentálásnak.

12. A központi számítógépek és a hálózat munkaállomásainak működésbiztonsága

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

12.1. Hálózat (LAN)

Az informatikai strukturált hálózat biztosítja a helyi LAN eszközök adatforgalmát. Ez magágan foglalja a munkaállomások, szerverek, hálózati tárolók, IP telefonok, Nyomtatók (MFP-k). A hálózatra tilos nem regisztrált, nyilvántartásban nem szereplő idegen gépek csatlakoztatása! Ennek biztosítása érdekében csak a regisztrált hardware elemeknek szabad hálózati hozzáférést (IP címet) biztosítani.

12.2. Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak egyeztetés után a rendszergazda engedélyével lehet.

Az interneten történő böngészés csak a munkához szükséges oldalak megtekintéséhez engedélyezett a munkahelyi LAN hálózaton.

A munkaállomásokat a bekapcsolási jelszóval kell védeni, melyet a felhasználó dokumentál.

A munkaállomás operációs rendszerét szintén jelszóval kell védeni. Bonyolultságát tekintve legalább 8 karakter hosszú, kis és nagybetűket, számot tartalmazó jelszavak használata kötelező és **legalább 6 havonta** meg kell változtatni!

A felhasználóknak a saját jelszavait dokumentálni kell lezárt, átvilágíthatatlan borítékban a 6.sz. melléklet alapján. A lezárt borítékon fel kell tüntetni a felhasználó nevét és a lezárás időpontját. A borítékot zárt helyen a munkáltató tárolja. Amennyiben szükséges a boríték felbontása (a felhasználó hirtelen betegsége, baleset, stb... miatt), azt a borítékon dokumentálni kell.

- Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

- Vírusfertőzés gyanúja esetén az arra illetékest (rendszergazdát) azonnal értesíteni kell.

- A fertőzött gépet azonnal le kell választani a számítógépes hálózatról, vagy minél előbb áramtalanítani!
- Vírusmentesítő programot futtatni csak felügyelet mellett szabad.
- Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
- Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
- A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
- Az informatikai eszközt és tartozékait helyéről elvinni engedélye nélkül nem szabad.
- A mobil eszközök épületből történi alkalomszerű és rendszeres kiviteléhez vezetői engedély szükséges, ami meghatározott időpontra, vagy időszakra szól. Lásd melléklet.

12.3. Weboldal működése

Az intézmény egy honlapot működtet több domain fenntartásával: www.egészség-prevencio.hu, www.gesz.szombathely.hu, www.efi.szombathely.hu

Az intézmény teljes honlapjának tekintetében **adatfelelős és egyben adatközlő szerepkört tölt be** az általános titkár, továbbá adatközlő még a titkársági asszisztens és a rendszergazda. Az intézményi honlapon belül működő Egészségfejlesztési Iroda oldalai tekintetében **adatfelelős** az iroda vezetője, **adatközlő** az iroda kijelölt munkatársa.

Az **adatfelelősök** kötelesek az adatokat előkészíteni, azokat pontos és naprakész állapotban tartani és az adatközlőnek eljuttatni. Az adatfelelősök a felsorolt kötelezettségeiket teljesítik, a megküldött adatok közzétételéért, folyamatos hozzáférhetőségéért és a közzétett adatok megküldöttek szerinti frissítéséért már az **adatközlők** felelnek. Az adatközlő feladata továbbá biztosítani, hogy az általa közzétett adatok megegyezzenek az adatfelelős által megküldött adatokkal. Azt, hogy a közzétett adatok azonosak-e az átadott adatokkal, valamint azt, hogy a közzétett adatok mennyire pontosak, időszerűek stb. az adatfelelős köteles ellenőrizni.

Amennyiben szükséges külső kommunikációs adatbázis: az adatfelelős naprakész elektronikus nyilvántartást vezet a külső kommunikációról, valamint megőrzi azok papír alapú dokumentációját is.

Az adatfelelős, valamint az adatközlő munkatársak munkaköri leírásában az intézmény igazgatója a betöltött szerepköröket nevesíti.

13. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy azok megismétlődjenek.

A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

Szombathely, 2024. január 01.

Vigné Horváth Ilona
igazgató

1. sz. melléklet

ADATKEZELÉSI NYILATKOZAT

Alulírott.....
(név ,lakcím)
nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető, a munkavégzéshez szükséges adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek.

Az informatikai eszközök háttértárolóján csak a munkavégzéshez szükséges adatok, fájlok programok tárolhatók, különös tekintettel tilos bármilyen illegális tartalom, médiatartalom letöltése, tárolása és felhasználása.
Az adatbiztonság, és jogszerű adattárolás megtartásáért az informatikai eszköz mindenkori kezelője a felelős személy.

A fentieket megértettem, büntetőjogi felelősségem tudatában magamra nézve kötelezőnek tartom.

Dátum: 20.....

.....
aláírás

2. sz. melléklet

Informatikai eszközzel ellátott helyiségek rendje

1. Az informatikai eszközzel ellátott helyiségekben az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:
   - az intézmény igazgatója, helyettesei
   - csoportvezetők
   - az igazgató által kijelölt személyek
   - rendszergazda
   - szolgáltatás jellegéből adódó helyeken az egészségügyi szolgáltatást igénybe vevő
   - munkavégzés céljából más tevékenység miatt megbízott vállalkozó, vagy annak alkalmazottja felügyelettel!
   - ügyintézés céljából a GESZ-el kapcsolatban lévő vállalkozók, intézményi dolgozók vagy alkalmazottai felügyelettel!

2. Munkaidő alatt az ajtókat állandóan becsukva, munkaidőn kívül pedig zárva kell tartani.

3. Munkaidőn kívül munkavállaló csak az intézmény igazgatójának (távollétében helyettesének) engedélyével tartózkodhat.

4. A munkaidő végén, a helyiséget utoljára elhagyó dolgozó köteles ellenőrizni az áramtalanítást, ellenőrizni az ablakok zárt állapotát, köteles a riasztóberendezést élesíteni és az ajtókat kulcsra zárni.

5. Az számítógéppel ellátott helyiségekben az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni.

6. A számítógépek közvetlen közelében ételt, italt fogyasztani TILOS!

7. A számítógéppel ellátott helyiségek takarítását arra kioktatott személyek végezhetik.

8. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak arra felhatalmazott rendszergazda végezhet. Ez alól csak a megbízott szervizek szakemberei kivételek – a megbízást írásos megrendelővel kell alátámasztani.

8. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az üzemszerű munkák elvégzésére lehet használni.

9. Az számítógéppel ellátott helyiségekben elhelyezett adathordozókhoz *az adatkezelő dolgozókon* kívül, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.

10.Optikai lemezeket, pendrive-okat, memóriakártyákat egyéb adathordozókat, valamint nyomtatványokat, dokumentumokat csak az adatkezelő engedélyével lehet kihozni, illetve bevinni a számítógéppel ellátott helyiségbe. Munkavégzés után ezeket a tárolási helyükre el kell zárni!

12. A Szünetmentes elektromos hálózatba csak számítógépeket és azok tartozékait lehet csatlakoztatni! Nyomtatókat szigorúan tilos!

13. A javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a szakszerűséget, a vonatkozó érintésvédelmi szabványokat és az esztétikai követelményeket.
Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

3. sz. melléklet

Informatikai biztonsági útmutató

Az intézmény informatikai szoftver-hardver védelmének eszközeit az Informatikai Biztonsági Szabályzat (IBSZ) foglalja magában. Ez minden dolgozó számára kötelező érvényű. Az IBSZ hozzáférhető az igazgatói irodában és a mindenki számára elérhető publikus hálózati tárhelyen. „Informatikai biztonsági útmutató" az IBSZ mellékletét képezi.
Az informatikai rendszer biztonsága érdekében a következő veszélyforrásokra kell különösen ügyelni:

1. **Külső adathordozókról történő adatátvitel** a számítógép háttértárolójára (CD-ről, pendrive-ról, stb.). Minden esetben az állomány megnyitás, másolás előtt kötelező a víruskeresés.
2. **Internet weboldalak megnyitása munkahelyi LAN hálózaton:** Csak a biztonságos adattartalommal rendelkező, illetve a munkavégzéshez kapcsolódó, vagy belső hálózaton tárolt intézményi weboldalakat szabad megnyitni. Szigorúan tilos az illegális fájlcserélő („torrent"), tiltott tartalommal rendelkező weblapok megnyitása, különös tekintettel a médiatartalmakra (mp3, filmek, képek).
3. **Veszélyes állományok**, melyek vírusokat hordozhatnak:
    - audio: MP3, WAV, stb.
    - video: AVI, MPG, MP4, WMV, MKV, stb.
    - kép: JPG, PNG, BMP, stb.
    - tömörített tartalmak: zip,arj,rar,7zip
    - alkalmazások: exe, jar,stb.
4. A nem beazonosítható úgynevezett **hivatkozás (link)** megnyitása nagy veszélyt rejt magában, mivel olyan káros tartalmú internetes oldalra irányíthat, ami vírust, kártevőt tartalmaz. Ezek a hivatkozások lehetnek weblapokon, megkaphatók e-mailben, chat site-okon vagy akár skype-on, messenger-en és más üzenetküldőn.
5. Csak olyan **e-mailt** nyissunk meg, melynek feladója beazonosítható, viszont ebben az esetben is óvatosan kell eljárni, mert egyes esetekben adathalász weboldalak, „cégek" saját ismerősünk által küldött üzenetként megjelenő e-mailjei is előfordulnak a postafiókunkban. Az ilyen e-mailek a gyanútlan felhasználót a bennük található linkre, vagy gombra kattintásra utasítják, amit követően azonnal indul a vírus, kémprogram telepítése a számítógépre. Amennyiben gyanús levelet kapunk azonnal töröljük és a törölt elemek közül is távolítsuk el. E-mail-ben kapott csatolt állományt semmiképpen ne nyissuk meg közvetlenül. Először a Fájl mentése lehetőséggel mentsük a számítógép háttértárolójára egy külön mappába, majd a megnyitása előtt víruskeresést kell rajta végrehajtani.
6. A **Vírusvédelem** hatékony működése érdekében automatikusan frissülnek a vírusvédelmi adatbázisok. Ha ez nem történne meg, a keresőprogram figyelmeztet. A vírusvédelem hiányáról az operációs rendszer ad figyelmeztetést. Ezeket az eseteket haladéktalanul jelezzük a rendszergazdának!

Összefoglalva a veszélyforrások:

- nem biztonságos weblap
- külső adathordozók
- veszélyes hivatkozások!!!
- e-mail-ek, különös tekintettel a csatolt állományokra
- nem működő vírusvédelem

Az intézmény tulajdonában lévő számítógépek háttértárolóján csak a munkavégzéshez szükséges adatok, fájlok programok tárolhatók, különös tekintettel tilos bármilyen illegális tartalom, médiatartalom letöltése, tárolása és felhasználása.
Az adatbiztonság, és jogszerű adattárolás megtartásáért a számítógép kezelője, felhasználója a felelős személy.

4. sz. melléklet

Informatikai eszközök kiviteli engedélye

Az alább felsorolt informatikai eszköz(ök) rendeltetésszerű tárolási helyétől eltérő helyre történő kivitelét

egyszeri alkalomra / meghatározott időtartamra

indoklás alapján engedélyezem:

	Megnevezés	Gyári szám	Indoklás

A felhasználó anyagi fellelőséggel tartozik az eszközben keletkezett károkért, abban az esetben, ha bizonyítottan saját hibájából történt a károkozás.

Engedélyezett időpont(ok) / időtartam:

_____

_____

_____

Szombathely, _____

_____

Vigné Horváth Ilona
igazgató

5. sz. melléklet

Engedélyezett informatikai alkalmazások

	Alkalmazás / programrendszer megnevezése	Leírás, megjegyzés	Használat kezdete / vége
1.	KIRA	Központosított Illetmény-számfejtési Rendszer intézményi modulja. A munkaállomásokon való működés alapfeltétele az intézmény-specifikus kulcsállomány megléte. A kulcsállomány archiválásra került optikai adathordozóra, így fájlsérülés esetén reprodukálható; csakúgy, mint a telepítő állományok. Az adatbázis mentése a központi számfejtési szerv a Magyar Államkincstár feladata, mivel fizikailag ez a központi szerveren helyezkedik el. A KIRA működésének másik alapfeltétele a mindenkori internet kapcsolat biztosítása.	
2.	AndIT Tárgyieszköz nyilvántartó	A Tárgyieszköz analitikus nyilvántartó program	
3.	AndIT Készletnyilvántartó	Készletet nyilvántartó program	
4.	AndIT Költségfelosztó	A tovább számlázandó közüzemi és egyéb számlák felosztásának számítására készített program	
5.	GORDIUS	pénzügyi információs rendszer, a Korend Rendszerház Kft által fejlesztett program. A rendszer az önkormányzat fájlszerverén helyezkedik el. Elérése távoli asztali kapcsolattal történik. A rendszer integrált funkciókkal rendelkezik, számlázó programként használható. Az GORDIUS Pénzügyi Információs Rendszer adatbázis mentését a Polgármesteri Hivatal Informatikai Irodájának - a központi adatbázisszerverhez rendszergazdai joggal rendelkező - megbízott dolgozója végzi.	
6	Visual SZOLGA	HIP Kft által kifejlesztett rendszer integrált egészségügyi informatikai rendszer, mely az egészségügy teljes	

		területén lefedi az alapellátási rendszert.	
7.	MED-MAX háziorvosi szoftver	A Profix Kft által fejlesztett rendszer, amit – egy kivétellel - egységesen minden háziorvosi szolgálat használ. Adatkezelésre, adatbázist kezelésre hálózatos üzemeltetésre alkalmas. Az egységességéből kifolyólag átjárhatóságot biztosít a rendszerek között – adatexport, adatimport -. GDPR megfelelőséget biztosítja, biztonságos üzemeltetést garantál.	2019. május
8.	STEFÁNIA	A Vitarex Stúdió Kft védőnői és iskolaorvosi dokumentációs és jelentő rendszer. Gépenként külön adatbázissal dolgozik.	
9.	OTP Electra	Az OTP Bank által biztosított ügyfélprogram.	
10.	TETFOG	A NEAK által ingyenesen rendelkezésre bocsátott tételes fogászati ellátásokat nyilvántartó és jelentő program.	
11.	GEKKOSOFT	Fogászati ellátások nyilvántartó TETFOG program EESZT interfész alkalmazása.	
12.	IRMA	Önkormányzat által rendelkezésre bocsátott elektronikus iktató program az teljes körű iratkezelés támogatására.	
13.	NOD32	Vírus és kémprogram kereső program, állandó felügyelettel, automatikus frissítéssel. Központilag felügyelhető vállalati licensz. Minden használatban lévő gépre kötelezően telepíteni kell.	
14.	Microsoft Office programcsomag	Microsoft termékcsomag, szöveg, táblázat, prezentációs dokumentumok előállítására, kezelésére. Elektronikus levelezés	
15.	Open Office	Nyílt forráskódú ingyenes dokumentum kezelő programcsomag.	
16.	Teamviewer	Távoli asztal szolgáltatást nyújtó segédprogram. Azon eszközökre telepítve, melyeknél előfordul a távsegítség igénye. Használata körültekintést igényel, a legszigorúbb biztonsági beállításokkal engedélyezett	GESZ licensz, évente megújuló

		csak a használata.	
17.	Google böngésző	Engedélyezett web-böngésző, igény szerint telepíthető	
18.	Mozilla Firefox böngésző	Engedélyezett web-böngésző, igény szerint telepíthető	
19.	Safari böngésző	Engedélyezett web-böngésző, igény szerint telepíthető	
20.	Internet Explorer böngésző	Engedélyezett web-böngésző, igény szerint telepíthető	
21.	Edge böngésző	Engedélyezett web-böngésző, igény szerint telepíthető	
22.	WinRAR	Tömörítő program, igény szerint telepíthető	
23.	OUTLOOK levelező rendszer	A hivatali email fiókok használatához Csak az alábbi szolgáltatói fiókok kezelésére: - minden @eu.savaria.hu - minden @gesz.szombathely.hu - efi@gmail.com - geszszombathely@gmail.com	
24.	Mozilla Thunderbird levelező rendszer	A hivatali email fiókok használatához Csak az alábbi szolgáltatói fiókok kezelésére: - minden @eu.savaria.hu	

6. sz. melléklet

Informatikai rendszerek, alkalmazások belépéséhez szükséges azonosító adatok

A használatos jelszavak kötelező módosítási periódusa **6 hónap**!
Az eszközök által megengedetten legalább 8 karakter hosszú, kis és nagy betűt és számjegyet kell tartalmaznia a jelszavaknak!

Felhasználó neve	***Munkahely, beosztás***	***Kelt***

Rendszer / Alkalmazás	***Felhasználónév***	***Jelszó***
Számítógép/eszköz bekapcsolási		
Operációs rendszer		

A nyilvántartást lezárt, átvilágíthatatlan borítékban, elzártan kell tárolni az erre rendszeresített helyen, az intézmény páncélszekrényében!
A borítékon csak a felhasználó nevét kell és a lezárás dátumát feltüntetni!
Felbontás esetén fel kell jegyezni a borítékra az időpontot és a bontás indokát!