EGRI HITTUDOMÁNYI FŐISKOLA

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT



Hatályos 2022.szeptember 6. napjától.

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

# A szabályzat célja

* + - 1. **(1)** Az Információbiztonsági Szabályzat (a továbbiakban: Szabályzat) alapvető célja, hogy az Egri Hittudományi Főiskolán (a továbbiakban: Főiskola) az informatikai rendszer kiépítése és működése során biztosítsa az adatvédelem elveinek, az információbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.
         1. A 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.

* + - * 1. A Szabályzatban meghatározott védelem a rendszerek tervezésének megkezdésétől az üzembehelyezésen keresztül az üzemeltetés teljes tartama alatt biztosítandó.

# A Szabályzat hatálya

* + - 1. **(1)** A Szabályzat személyi hatálya kiterjed a Főiskola minden munkatársára és hallgatójára, valamint azokra a személyekre, akik eseti engedéllyel használják a Főiskola számítógép hálózatát vagy informatikai eszközeit, berendezéseit. Az eseti engedély megadása előtt be kell szerezni az érintett nyilatkozatát arról, hogy a Szabályzat rendelkezéseit magára nézve kötelezőnek ismeri el a Főiskola számítógép hálózatán, illetve informatikai eszközein, berendezésein végzett munka vonatkozásában.
         1. A Szabályzat tárgyi hatálya kiterjed

a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül;

a Főiskola tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint az informatikai eszközök műszaki dokumentációira;

az informatikai folyamatok összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési);

a rendszer- és felhasználói programokra;

az adatok felhasználására vonatkozó utasításokra;

az adathordozók tárolására és felhasználására.

# A Szabályzat alkalmazásának módja

* + - 1. A Szabályzat megismerését az érintett dolgozók részére a vezetők és a rendszergazda oktatás formájában biztosítja. A Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az Szabályzat előírásainak megfelelően.

# A Szabályzat karbantartása

* + - 1. A Szabályzatot az informatikában a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. A Szabályzat folyamatos karbantartása az intézmény vezetésének feladata, amelyben a rendszergazda közreműködik.

# Az adatkezelés során használt fontosabb fogalmak

* + - 1. A Szabályzat alkalmazásában:

1. **Adatállomány:** Az egy nyilvántartásban kezelt adatok összessége.
2. **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.
3. **Adatfeldolgozás:** Az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.
4. **Adatfeldolgozó:** Az a természetes vagy jogi személy, aki, vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.
5. **Adatfelelős:** Az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.
6. **Adatkezelés:** Az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is.
7. **Adatkezelő:** Az a természetes vagy jogi személy, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.
8. **Adatközlő:** Az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi.
9. **Adatmegjelölés:** Az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.
10. **Adatmegsemmisítés:** Az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.
11. **Adattovábbítás:** Az az eljárás, amely során az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.
12. **Adattörlés:** Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
13. **Adatzárolás:** Az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.
14. **Érintett:** bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.
15. **Harmadik személy:** Olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.
16. **Hozzájárulás:** Az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.
17. **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, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.
18. **Közérdekből nyilvános adat:** A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
19. **Különleges személyes adat:**
    1. a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat;
    2. az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.
20. **Nyilvánosságra hozatal:** Az adat bárki számára történő hozzáférhetővé tétele.
21. **Személyes adat:** Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés.
22. **Tiltakozás:** Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

# Az információs rendszerek biztonsági fokozatba sorolása

* + - 1. **(1)** A Főiskola az információs rendszerei biztonsági szintbe és osztályba sorolását az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben foglalt osztályozási rendszer szerint végzi.
         1. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A kezelt adatok és a funkciók figyelembe vételével a lehetséges kármértéket kell megállapítani, míg a kár bekövetkezésének valószínűsége a körülmények mérlegelésével becsülhető.
         2. Azokban az esetekben, amikor a Főiskola külső szolgáltatót vesz igénybe, a biztonsági osztályba sorolás a szolgáltató feladata, amelyről a Főiskola tájékoztatást kell, hogy kérjen. A kockázatelemzés és kockázatkezelés során a Főiskolának figyelembe kell vennie a külső szolgáltató által meghatározott biztonsági osztály értékét.
         3. A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5- ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt. Az elektronikus információs rendszer biztonsági osztálya alapján kell megvalósítani az előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.
         4. A Főiskola rektora hagyja jóvá a biztonsági besorolást.

# A védelem tárgya

* + - 1. A védelmi intézkedések kiterjednek:

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 a szellemi alkotások tekintetében.

# A védelem felelőse

* + - 1. **(1)** A védelem felelőse a mindenkori rendszergazda.
         1. A Szabályzatban foglaltak szakszerű végrehajtásáról a Főiskola vezetése gondoskodik.

## A védelmi felelősök feladatai

* + - 1. Az intézményi vezetés feladatai:

a Szabályzat kezelése, naprakészen tartása, módosítások átvezetése;

meghatározza a védett adatok körét;

ellátja az adatkezelés és adatfeldolgozás felügyeletét;

ellenőrzi a védelmi előírások betartását;

az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása;

az adatvédelmi feladatok ismertetése;

ellenőri tevékenységét adminisztrálja;

ellenőrzi a szoftverek használatának jogszerűségét.

* + - 1. A rendszergazda feladatai:

a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli;

felelős az informatikai rendszerek üzembiztonságáért, karbantartásáért, a szerverek adatairól való biztonsági másolatok készítéséért;

gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról;

folyamatosan ellenőrzi a védelmi eszközök működését;

felelős az informatikai rendszer hardver eszközeinek karbantartásáért;

nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket;

gondoskodik a folyamatos vírusvédelemről;

a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről;

folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását;

javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására;

ellenőrzi a rendszer adminisztrációját, részt vesz a Szabályzat napra készen tartásában.

* + - 1. Felhasználó feladatai:

az általa létrehozott adatok mentésének biztosítása;

hozzáférési azonosítói és a hozzájuk tartozó jelszavak titkosságának megőrzése.

# A védelem eszközei

* + - 1. 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.

# Védelmet igénylő, az informatikai rendszerre ható elemek

* + - 1. 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.

# A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

* + - 1. **(1)** Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

közlésre szánt, bárki által megismerhető adatok;

bizalmas, személyes adatok;

minősített, titkos adatok.

* + - * 1. Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik. Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot, abban a terjedelemben, amelyben az adatok megismerésére a munkavégzéshez szükség van. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell. Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy adathordozóra történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető. A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a Főiskola vezetése felé jelenteni kell. A naplófájlok áttekintéséért, értékeléséért az intézményi vezetés és a Rendszergazda a felelősek. Az 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 is biztosítani kell (szoftver, hardver adatvédelem).

# Az informatikai eszközbázist veszélyeztető helyzetek

* + - 1. **(1)** 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.
         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.

* + - * 1. 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 megváltozott körülmények figyelmen kívül hagyása,

vírusfertőzött adathordozó behozatala,

biztonsági követelmények és gyári előírások be nem tartása,

adathordozók megrongálása (rossz tárolás, kezelés),

a karbantartási műveletek elmulasztása.

* + - * 1. A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

# Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

* + - 1. **(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.

* + - * 1. A rendszerek megvalósítása során előforduló veszélyforrások:

hibás adatállomány működése,

helytelen adatkezelés,

programtesztelés elhagyása.

* + - * 1. A működés és fejlesztés során előforduló veszélyforrások:

emberi gondatlanság,

szervezetlenség,

képzetlenség,

szándékosan elkövetett illetéktelen beavatkozás,

illetéktelen hozzáférés,

üzemeltetési dokumentáció hiánya.

# Az informatikai eszközök környezetének védelme

## Vagyonvédelem

* + - 1. Vagyonvédelmi előírások:

a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni;

a gépterembe való be- és kilépés rendjét szabályozni kell;

a gépterembe, szerverterembe történő illetéktelen behatolás tényét a Főiskola vezetésének azonnal jelenteni kell;

az informatikai eszközöket csak a Főiskola arra felhatalmazott alkalmazottai használhatják;

az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

* + - 1. Az adathordozók fizikai kezelése:

könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;

az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni;

a használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni;

a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek;

adathordozót másnak átadni csak engedéllyel szabad;

a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

## Tűzvédelem

* + - 1. A gépterem, illetve kiszolgáló helyiségei a „D” tűzveszélyességi osztályba tartoznak, amely mérsékelten tűzveszélyes üzemet jelent. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. A géptermekbe, szerverszobákba minimum 1-1 db tűzoltó készüléket kell elhelyezni. A géptermekben, szerverszobákban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, illetve engedélyével szabad végezni. A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok körének meghatározása a Főiskolai vezetés hatásköre.)

# Az informatikai rendszer alkalmazásánál felhasználandó védelmi eszközök és módszerek

## A számítógépek és szerverek védelme

* + - 1. Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

menteni a még használható anyagot,

biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,

archivált anyagok (eszközök) használatával folytatni kell a feldolgozást.

## Hardver védelem

* + - 1. **(1)** A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik. A munkák szervezésénél figyelembe kell venni:

a gyártó előírásait, ajánlásait;

a tapasztalatokat.

* + - * 1. Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

## Az informatikai feldolgozás folyamatának védelme

* + - 1. **(1)** Az adatrögzítés védelme:

az adatbevitel hibátlan műszaki állapotú berendezésen történjen;

az adatállomány rögzítése tesztelt adathordozóra történjen;

a bizonylatok és adathordozók tárolása csak e célra kialakított és megfelelő tároló helyeken történjen;

* + - * 1. Az adatrögzítő szoftver védelme:

lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal, és

biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.

* + - * 1. Hozzáférési lehetőség:

a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz;

azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti;

a szerverek rendszergazdai jelszavát a vezető rendszergazda kezeli.

* + - * 1. Az adatrögzítés folyamatához kapcsolódó szabályozó dokumentumok:

adatrögzítési utasítások,

ellenőrző rögzítési utasítások,

tesztelő és törlő programok kezelési utasításai,

megőrzési utasítások,

gépkezelési leírások.

* + - * 1. Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.
        2. Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.
        3. Az adathordozók megőrzési idejét a jogszabályokban meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani.
        4. A selejtezést a Főiskola selejtezési szabályzata alapján kell lefolytatni.
        5. Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.
        6. A szoftvereket és adathordozókat a Főiskola leltározási szabályzatában foglaltaknak megfelelően kell leltározni.
        7. Az adatfeldolgozás után biztosítani kell az adatok mentését. A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata. A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban a rendszergazda nyújt segítséget. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda a felelős.

## Szoftver védelem

* + - 1. **(1)** Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.
         1. A felhasználó programok kezelése folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.
         2. A programokról a leltárfelelősnek naprakész nyilvántartást kell vezetni. A számvitelről szóló többször módosított 2000. évi C. törvény szerint a nyilvántartást olvasható formában legalább 10 évig meg kell őrizni. A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét. A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

## Az internethasználat biztonsága

* + - 1. Az internethasználat körében a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) 6. § (2) bekezdése szerinti jóhiszeműség és tisztesség elvén, valamint az 52. § (1) bekezdésében tárgyalt munkavállalói kötelezettségek keretei között a Főiskola a következő szabályok megtartását várja el különösen a Főiskolán, annak tulajdonában álló számítástechnikai eszközön, illetve a Főiskola informatikai hálózatának igénybevételével végzett tevékenység során:

tilos a szervezettel kapcsolatos információk nyilvános internetes oldalakon való engedély nélküli közzététele;

tilos egyes interneten megvalósuló tevékenységek végzése (chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem támogatott levelezőlisták, privát levelezési fiók munkaköri használata);

elvárt a Főiskola partnerei adatainak bizalmas kezelése;

elvárt, hogy a munkatárs a közösségi médiában tiszteletben tartsák a Főiskola szellemiségét, reputációját, megítélését, ne tegyen olyan cselekedetet, ami sértheti azt;

elvárt a szellemi tulajdonra vonatkozó szabályok betartása;

nem engedélyezett a munkakör feladatellátásához nem szükséges kép- és videóanyag letöltése;

tilos szórakoztató és játék alkalmazások használata.

## Az e-mail használat biztonsága

* + - 1. **(1)** Minden munkatárs egyedi főiskolai elektronikus levelezési cím használatára jogosult, ami részére.
         1. A Főiskola elektronikus levelező rendszere elsődlegesen a főiskolai belső- és külső kommunikációt, valamint a belső folyamatok támogatását szolgálja.
         2. Az elektronikus levelezés tekintetében a Főiskola fenntartja a jogot arra, hogy – kizárólag indokolt esetben, a munkatárs előzetes tájékoztatása mellett – betekintsen az elektronikus levelekbe ellenőrzés céljából, továbbá hogy a felhasználók levelezési forgalmát figyelje, naplózza. A betekintés során a munkáltató kizárólag a munkavégzéssel összefüggő levelezések tartalmát ismerheti meg, az esetleges magáncélú levelek tartalmába nem tekinthet be. A munkatársnak a postafiókban a magáncélú leveleket elkülönített módon kell tárolnia. A felhasználók tudomásul veszik, hogy az általuk küldött és fogadott elektronikus küldeményeket a Főiskola ilyen módon kezeli.
         3. Az elektronikus levelezési rendszerbe beérkező leveleket minden esetben ellenőrizni kell, hogy nem tartalmaznak-e valamilyen, a Főiskola informatikai rendszerét veszélyeztető programot, kódrészletet, scriptet.
         4. A főiskolai elektronikus levelező rendszer használata során a felhasználó számára tilos:

a hivatalosan támogatott elektronikus levelező szolgáltatáson (szerveren) kívül más elektronikus levelező szolgáltatást hivatalos levelezésre használni;

a hivatalosan támogatott levelező szoftveren kívül más programot használni;

az elektronikus leveleket úgy titkosítani, hogy a visszafejtésre használható kulcs nincs, vagy nem kerülhet a Főiskola birtokába;

a Főiskola hálózatát vagy szervereit nagy terjedelmű vagy nagy mennyiségű levél, illetve kéretlen kereskedelmi üzenetek küldésére használni (ha ilyenre van szükség, akkor azt a rendszergazda bevonásával más technológia alkalmazásával kell teljesíteni);

ügyviteli szempontból titkos, bizalmas, illetve belső információk jogosulatlan nyilvánosságra hozatala;

a Főiskola levelezési rendszeréből a szervezeten kívülre olyan információkat kijuttatni, amelyek kijuttatására a felhasználó más csatornán sem jogosult;

a levelezőrendszert reklám célra, pártpolitikai célra, mások munkájának hátráltatására, illetve az internet veszélyeztetésére használni;

a Főiskola hálózatát vagy szervereit kéretlen, nagy mennyiségű, illetve kereskedelmi elektronikus levelekre való válaszok begyűjtésére használni;

indokolatlanul nagy méretű üzeneteket vagy fájlokat küldeni;

láncleveleket vagy hasonló üzeneteket küldeni, tovább küldeni;

vírusos levelek szándékos küldése, továbbküldése;

válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a Főiskola biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást;

az e-mailben csatolt futtatható állományok megnyitása/letöltése a munkaállomásokra;

ismeretlen feladótól származó levelekben található csatolmány megnyitása;

valótlan információt hordozó levelek tudatos továbbítása;

az elküldött levél járulékos adatainak (például feladó e-mail címe, küldés időpontja) meghamisítása;

a munkatársak e-mail címeinek másik félhez történő, jogosulatlan továbbítása;

a főiskolai e-mail címről magáncélú regisztrációt végrehajtani (pl. üzleti célú levelezési listákra, fórumokra, hírcsoportokra feliratkozás);

privát postafiók tartalom automatikus továbbítása a főiskolai e-mail címre;

a Főiskola elektronikus levelezési címjegyzékének kiadása harmadik fél számára;

nyilvános levelezési fórumokon a Főiskolánál regisztrált levelezési cím feltüntetésével állást foglalni;

a főiskolai levelezési cím feltüntetésével, illetve annak használatával – a Főiskola érdekeinek megvalósulását kifejezetten segítő feladatokat kivéve – bármilyen kereskedelmi, hirdetési tevékenységben részt venni;

a főiskolai levelezési cím feltüntetésével feliratkozni nem szakmai jellegű, illetve nem az ügyviteli vagy oktatási munkát segítő hírlevélküldő szolgáltatásra.

## Személyi információbiztonság a munkavégzési helyen

* + - 1. A napi munkavégzés során:

a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről;

a felhasználó a számítógépét zárolni köteles, ha azt rövidebb időre őrizetlenül hagyja;

hosszabb idejű távollét esetén a számítógépből ki kell jelentkezni, illetve ki kell azt kapcsolni (amennyiben lehetősége van, áramot is lekapcsolni);

a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a számítógépet;

munkavégzés után minden védendő adatot tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) el kell tenni az asztalokról, és zárható irodabútorban kell tárolni;

gondoskodni kell arról, hogy a nyomtatókból, faxokból, fénymásolóból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá;

védendő adatot tartalmazó dokumentum ne maradjon a fénymásolóban;

illetéktelen személy nem tartózkodhat felügyelet nélkül az irodában;

az iroda elhagyásakor az irodaajtót kulccsal kell zárni;

hulladékgyűjtő edényben védendő adatot tartalmazó dokumentumot vagy annak piszkozatát elhelyezni csak iratmegsemmisítővel felismerhetetlenné tett állapotban szabad.

## Személyi információbiztonság a jogviszony megszűnésekor, megszüntetésekor vagy módosításakor

* + - 1. **(1)** A jogviszony megszűnése, megszüntetése a felhasználói hozzáférés jogainak teljes visszavonását követeli meg a Főiskola információs rendszereiben.
         1. Jogviszony megszűnése esetén, legkésőbb a jogviszony megszűnésének napján a rendszergazda – biztonsági szempontból – minden informatikai jogosultságot megvon a jogosulttól a Gazdasági Hivatal előzetes jelzése alapján, így különösen:

elektronikus levelezési fiók használati jogosultsága;

a használt informatikai rendszerek rendszergazdai, felhasználói jogosultságai.

* + - * 1. Jogviszony megszűnése esetén, legkésőbb a jogviszony megszűnésének napján kötelező a használatba adott mobil eszközök (asztali, illetve hordozható számítógép, telefon) visszaszolgáltatása a rendszergazdánál, aki azok használhatóságát ellenőrzi. A kilépő dolgozó a leadásra kerülő eszközök jelszóvédelmét köteles feloldani.
        2. Jogviszony módosítása, munkakör megváltozása esetén gondoskodni kell arról, hogy az érintett a változást követően csak azon rendszerekhez és az abban kezelt adatokhoz férhessen hozzá, amelyek megismerésére, kezelésére a változást követően jogosult. A rendszergazda a jogviszony módosításának hatályba lépésével egyidejűleg a Gazdasági Hivatal jelzése alapján

módosítja vagy megszünteti a hozzáféréseket az addig használt rendszerekhez, illetve

megadja a hozzáféréseket azokhoz a rendszerekhez, amelyekhez addig nem volt hozzáférése az érintett személynek, de a jogviszony változásával a hozzáférésre jogosulttá válik.

* + - * 1. A Szabályzatnak a jogviszony megszűnés vagy módosítás esetén alkalmazandó szabályait a külső szolgáltatóval való jogviszony megszűnésének vagy változásának eseteiben is meg kell tartani.

# A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

## Központi gépek

* + - 1. Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftverekről biztonsági másolatot kell készíteni.

## Munkaállomások

* + - 1. Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell. Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket. A Főiskola informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül tilos. 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 csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

# Ellenőrzés

* + - 1. Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön. A munkafolyamatba épített ellenőrzés során a Szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

# Záró rendelkezések

* + - 1. **(1)** A Szabályzat a kihirdetését követő lép hatályba.
         1. A Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a Szabályzatban előírt feladatokat.

**Elfogadási záradék**

A jelen szabályzatot az Egri Hittudományi Főiskola Szenátusa a Szabályzatot 57/2022. számú határozatával elfogadta. Hatályba lép 2022. szeptember 7. napján.

Kelt Egerben, 2022. szeptember 06. napján.

Dr. Dolhai Lajos s. k.

rektor

a Szenátus elnöke