Apor Vilmos Katolikus Főiskola

Informatikai Biztonsági Szabályzat (IBSZ)

Apor Vilmos Katolikus Főiskola
Tudás. Hit. Jövő.

2025.

Az Apor Vilmos Katolikus Főiskola a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (GDPR) 2. szakasz 32. cikke, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § a, valamint a munka törvénykönyvéről szóló 2012. évi 1. törvény 5/A pontja alapján a következő szabályzatot alkotja:

1. § A szabályzat célja

(1) Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja, hogy az informatikai rendszer alkalmazása során biztosítsa a főiskola alkalmazottai, valamint hallgatói által kezelt adatok vonatkozásában az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

(2) Az IBSZ célja továbbá:

a) az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartatása,
b) az üzemeltetett számítógépek, informatikai eszközök, valamint a kamera- és beléptetőrendszer rendeltetésszerű használata,
c) a számítógépes rendszerek zavartalan üzemeltetése,
d) az üzembiztonságot szolgáló karbantartás és fenntartás,
e) az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre csökkentése,
f) az adatállományok tartalmi és formai épségének megőrzése,
g) a munkaállomásokon lekérdezhető adatok körének meghatározása,
h) az adatállományok biztonságos mentése,
i) a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
j) az adatvédelem és adatbiztonság feltételeinek megteremtése.

2. § A szabályzat hatálya

(1) Az IBSZ személyi hatálya kiterjed az Apor Vilmos Katolikus Főiskola (továbbiakban: AVKF) valamennyi alkalmazottjára és hallgatójára.

(2) Az IBSZ tárgyi hatálya kiterjed:

a) az AVKF tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációjára;
b) a rendszer- és felhasználói programokra;
c) a védelmet élvező adatok teljes körére, felmerülésük és feldolgozásuk helyétől, idejétől és az adatok fizikai megjelenési formájától függetlenül;
d) az adatok felhasználására, tárolására vonatkozó utasításokra;
e) az adathordozók tárolására, felhasználására.

3. § Értelmező rendelkezések

(1) Adat: a természetes vagy mesterséges objektumok, folyamatok, állapotok jellemzői, illetőleg azok részleteinek érzékelhető formában történő megjelenítése. Adat tágabb értelemben jelenthet szöveget, számot, rajzot, térképi részleteket vagy bármely más információt a megjelenési módjára vagy formájára való tekintet nélkül.

(2) Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

(3) Adatkezelés: az alkalmazott eljárástól függetlenül adatokon végzett bármely művelet vagy műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, felhasználása, összekapcsolása, szolgáltatása, megjelenítése stb.

(4) Adatkezelő: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.
(5) Adatvédelem: az adatokhoz való illetéktelen hozzáférés, a meghibásodás, a megsemmisülés stb. megakadályozása; a személyes adatok esetében kiegészül az adott személy személyes adatai jogellenes gyűjtése, kezelése, tárolása, felhasználása elleni védelemmel.
(6) Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
(7) Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.
(8) Információ: jelentéssel bíró adat, megjelenési módjára vagy formájára való tekintet nélkül.
(9) Informatikai rendszer: a főiskola számítógép-hálózata, beleértve hálózati eszközöket, szervereket, általános célú számítógépeket, laptopokat, projektorokat, felhasználói és rendszerszoftvereket, sokszorosító, digitalizáló berendezéseket és a telefonrendszert.
(10) Rendszergazda: az a számítástechnikai ismeretekkel rendelkező személy, akit ezzel a feladattal a felhatalmazott szervezeti egység vezetője írásban megbíz.
(11) A rendszergazda a számítógép hardver- és szoftverkarbantartását, -fejlesztését, hibáinak feltárását és – ha lehetséges – javítását végzi.

4. § Az IBSZ biztonsági fokozata

(1) Az IBSZ biztonsági fokozata az AVKF-nél alapbiztonsági fokozat. (Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az AVKF belső szabályozásában hozzáférés-korlátozás alá eső [pl. egyes feladatok végrehajtása érdekében bizalmas] és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.)

5. § Kapcsolódó szabályzatok

(1) Az IBSZ előírásai összhangban vannak:
a) a Szervezeti és működési szabályzattal,
b) a Leltározási és leltárkészítési szabályzattal,
c) a Felesleges vagyontárgyak hasznosítási és selejtezési szabályzatával,
d) a Kommunikációs szabályzattal,
e) a Tűzvédelmi szabályzattal,
f) az Adatvédelmi és adatbiztonsági szabályzattal.

6. § Védelmet igénylő, az informatikai rendszerre ható elemek

(1) Az informatikai rendszer egymással szervesen együttműködő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
(2) Az informatikai rendszerre az alábbi tényezők hatnak:
a) a környezeti infrastruktúra,
b) a hardverelemek,
c) az adathordozók,
d) a dokumentumok,
e) a szoftverelemek,
f) az adatok,
g) a rendszerelemekkel kapcsolatba kerülő személyek.

7. § A védelem tárgya

(1) A védelmi intézkedések kiterjednek:
   a) a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
   b) az alkalmazott hardvereszközökre és azok működési biztonságára,
   c) az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
   d) az adatokra és adathordozókra, a megsemmisítésükig,
   e) az adatfeldolgozó programrendszerekre, valamint rendszerszoftverek tartalmi és logikai egységére, reprodukálhatóságára,
   f) a személyhez fűződő és vagyoni jogokra.

8. § A védelem eszközei

(1) A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések.
(2) Azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó, kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

9. § Az informatikai biztonsági felelősök és a felhasználók feladatai

(1) Az informatikai vezető (IT vezető) feladatai:
   a) az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
   b) javaslatot tesz a rövid- és hosszútávú rendszerfejlesztésre,
   c) meghatározza a védett adatok körét,
   d) ellátja az adatkezelés és adatfeldolgozás felügyeletét,
   e) ellenőrzi a védelmi előírások betartását,
   f) együttműködik az adatvédelmi tisztviselővel.
(2) A rendszergazda feladatai:
   a) a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
   b) felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
   c) gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
   d) feladata a védelmi eszközök működésének folyamatos ellenőrzése,
   e) felelős az informatikai rendszer hardvereszközeinek karbantartásáért,
   f) nyilvántartja a beszerzett, illetve üzemeltetett hardver- és szoftvereszközöket,
   g) gondoskodik a folyamatos vírusvédelemről,
   h) a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
   i) folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából lényeges paraméterek alakulását,
   j) ellenőrzi a rendszer adminisztrációját,
   k) a felhasználók számítógépén ellenőrzi a szoftverek használatának jogszerűségét.
(3) A felhasználó feladatai
   a) az általa létrehozott adatok mentésének biztosítása,
   b) hozzáférési azonosítóinak és a hozzájuk tartozó jelszavai titkosságának megőrzése,
   c) jelen szabályzat rendelkezéseinek betartása.

10. § Az informatikai vezető ellenőrzéssel kapcsolatos feladatai

(1) Rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot.
(2) Előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

11. § Az informatikai vezető jogai

(1) Az informatikai vezető jogai:
a) Az előírások be nem tartása esetén felelősségre vonási eljárást kezdeményezhet a Rektornál,
b) bármely érintett szervezeti egységnél jogosult ellenőrzésre,
c) betekinthet az informatikai feldolgozásokkal kapcsolatos valamennyi iratba,
d) javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
e) adatvédelmi és adatbiztonsági szempontból véleményezi az informatikai beruházásokat.

12. § Az IBSZ megismerhetőségének és alkalmazásának módja

(1) Az IBSZ megismerését az érintett munkatársak és hallgatók részére a főiskola honlapján való közzététel formájában biztosítani kell.
(2) Az IBSZ által érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

13. § Az IBSZ felülvizsgálata

(1) Az IBSZ-t az informatikában, valamint az AVKF-nél bekövetkező változások miatt időközönként, de legalább évente egyszer felül kell vizsgálni, és szükség szerint aktualizálni.
(2) Az IBSZ folyamatos felülvizsgálata és aktualizálása az informatikai vezető feladata.

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

(1) Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:
a) közlésre szánt, bárki által megismerhető adatok,
b) bizalmas, személyes adatok,
c) minősített, titkos adatok.
(2) A különös védelmi utasításoknak és szabályozásoknak összhangban kell lenniük a hatályos jogszabályokkal.
(3) A hivatali és szolgálati titokkal kapcsolatos tájékoztatást az Adatvédelmi és adatbiztonsági szabályzat, illetve a munkaköri leírás tartalmazza.
(4) Mindenki csak ahhoz az adathoz férhet hozzá, amelyre a munkájához feltétlen szüksége van.
(5) Az információhoz való hozzáférést – lehetőség szerint a tevékenység naplózásával – dokumentálni kell, hogy bármely – számítógépen végzett tevékenység (adatbázisokhoz való hozzáférés, a fájlba, külső adathordozóra történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet) – utólag visszakereshető legyen.

(6) A jogosulatlan hozzáférés gyanújának felmerülését haladéktalanul jelezni kell a rendszergazdának és az informatikai vezetőnek. A bejelentések kivizsgálásáért az informatikai vezető és a rendszergazda a felelős.

15. § Hozzáférési jogosultságok

(1) A munkaszerződésben vagy a megbízási szerződésben rögzített munkafolyamatok ellátásához szükséges jogosultságokat a szerződés megkötése után a munkaügyi kollégák jelzése alapján az informatikus osztja ki a munkavállalóknak.
(2) A fentieken túlmutató hozzáférési jogosultsági igényt az igénylő személy szervezeti egységének vezetője és az AVKF rektora bírálja el, jóváhagyása szükségszerű.
(3) A beérkezett és elbírált hozzáférési jogosultságok kiosztását, illetve módosítását az Informatika erre a feladatra feljogosított munkatársai végzik.

16. § Az informatikai eszközbázist veszélyeztető helyzetek

(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.
(2) Veszélyeztető helyzetek lehetnek például:

a) Környezeti infrastruktúra okozta ártalmak
   a. elemi csapás,
      i. földrengés, árvíz,
      ii. tűz,
      iii. villámcsapás,
      iv. egyéb vis maior
   b. környezeti kár:
      i. légszennyezettség,
      ii. nagy teljesítményű elektromágneses mező,
      iii. elektrosztatikus feltöltődés,
      iv. a levegő nedvességtartalmának felszökése vagy leesése,
      v. piszkolódás (pl. por).
   c. közüzemi szolgáltatásban bekövetkező zavarok
      i. feszültségkimaradás,
      ii. feszültségingadozás,
      iii. elektromos zárlat,
      iv. csőtörés.

b) Emberi tényezőre visszavezethető veszélyek
   a. szándékos károkozás:
      i. illetéktelen behatolás az informatikai rendszerek környezetébe
      ii. illetéktelen hozzáférés (adat, eszköz)
      iii. adatok, eszközök eltulajdonítása
      iv. rongálás (gép, adathordozó)
      v. megtévesztő adatok bevitele és képzése
      vi. zavarás (feldolgozások, munkafolyamatok, hálózati forgalom)

b. gondatlan károkozás:
    i. figyelmetlenség (ellenőrzés hiánya)
    ii. szakmai hozzá nem értés
    iii. a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása
    iv. a megváltozott körülmények figyelmen kívül hagyása
    v. vírusfertőzött adathordozó behozatala
    vi. biztonsági követelmények és gyári előírások be nem tartása
    vii. adathordozók megrongálása (rossz tárolás, kezelés)
    viii. a karbantartási műveletek elmulasztása

(3) A szükséges biztonsági, jelző- és riasztóberendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.
(4) Károkozás esetén belső vizsgálatot kell lefolytatni, amelyet az erre a célra kijelölt eseti bizottság végez el.
(5) Szándékos károkozás esetén azonnal meg kell akadályozni minden további hozzáférést.
(6) A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 386.§-a szerinti „Védelmet biztosító műszaki intézkedés kijátszása", a Btk. 422. §-a szerinti „Tiltott adatszerzés", a Btk. 423. §-a szerinti „Információs rendszer vagy adat megsértése" vagy a Btk. 424. §-a szerinti „Információs rendszer védelmét biztosító technikai intézkedés kijátszása" bűncselekmény gyanújának fennállása esetén az AVKF feljelentést tesz az illetékes hatóság felé.
(7) A szándékos károkozás tényéről és a tett intézkedésről írásban kell tájékoztatni a főiskola Rektorát.
(8) Gondatlan károkozás esetén meg kell határozni a károkozó felelősségének mértékét, és annak függvényében kell lefolytatni a szükséges fegyelmi eljárást.

17. § Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

(1) A tervezés és az előkészítés során előforduló veszélyforrások:
    a) a rendszerterv nem veszi figyelembe az alkalmazott hardvereszköz lehetőségeit,
    b) hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.
(2) A rendszerek megvalósítása során előforduló veszélyforrások
    a) hibás adatállomány működése,
    b) helytelen adatkezelés.
(3) A működés és fejlesztés során előforduló veszélyforrások
    a) emberi gondatlanság,
    b) szervezetlenség,
    c) képzetlenség,
    d) illetéktelen beavatkozás,
    e) illetéktelen hozzáférés.

18. § Az informatikai eszközök környezetének védelme

(1) Vagyonvédelmi előírások
    a) a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
    b) a gépterembe való be- és kilépés rendjét szabályozni kell,
    c) a számítógép monitorát lehetőleg úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
    d) a gépterembe, szerverterembe történő illetéktelen behatolás tényét a rektornak és az informatikai vezetőnek azonnal jelenteni kell,
    e) az informatikai eszközöket csak a főiskola alkalmazottjai és hallgatói használhatják,

f) az informatikai eszközök rendeltetésszerű használatáért a felhasználó a felelős.

(2) Adathordozók
   a) könnyen tisztítható, jól zárható szekrényben kell elhelyezni, úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
   b) a használni kívánt külső adathordozót a tárolásra kijelölt helyről kell kivenni, és oda is kell visszahelyezni,
   c) a munkák befejeztével a használt eszközöket az eredeti tárolási helyre vissza kell tenni,
   d) adatállomány rögzítése csak tesztelt adathordozóra történhet.
   e) Az adathordozók tárolására a műszaki, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.
   f) Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvényben foglaltak, továbbá az AVKF Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

(3) Elektronikus adattovábbítás
   a) Az AVKF hálózatára a csatlakozás csak hálózati azonosító birtokában lehetséges.
   b) A hálózati azonosítókat, digitális aláírásokat központilag az Informatika osztja ki a munkatársak és a hallgatók részére.

(4) Tűzvédelem

A hatályos tűzvédelmi szabályzat szerint.

19. § Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

(1) A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor a keletkezett károk minimalizálása érdekében az alábbiakat kell sürgősen elvégezni:
   a) menteni a még használható anyagot,
   b) biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
   c) archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

(2) Hardvervédelem
   a) Az eszközök hibátlan és üzemszerű működését biztosítani kell.
   b) Az üzemeltetési, karbantartási és szervizelési feladatok ellátásáról az Informatika gondoskodik.
   c) A javítási munkák elvégzésekor figyelembe kell venni:
      a. a gyártó előírásait, ajánlatait,
      b. a költséghatékonyságot.
   d) Bármely számítógép vagy számítástechnikai eszköz szétbontását csak az Informatika munkatársa, vagy az informatikai vezető által kijelölt személy végezheti el. (Garanciális eszközök esetén a garanciális javítást végző szerviz munkatársa.)

(3) Leltározás

A szoftvereket és adathordozókat a Leltározási és leltárkészítési szabályzatban foglaltaknak megfelelően kell leltározni.

(4) Selejtezés, sokszorosítás, másolás
   a) A selejtezést a Főiskola Felesleges vagyontárgyai feltárásának, hasznosításának és selejtezésének szabályzata, valamint az Iratkezelési szabályzat és irattári terv alapján kell lefolytatni.
   b) Selejtezéskor biztonsági intézkedésekkel kell megakadályozni, hogy a hibás informatikai eszközök adathordozói ellenőrizetlenül kerüljenek ki a szervezeten kívülre.

c) Alapvető követelmény, hogy a selejtezés vezetői engedélyhez kötött és megfelelően dokumentált legyen. A selejtezési jegyzőkönyvben – a későbbi félreértések elkerülése végett – érdemes feltüntetni a selejtezendő eszköz leltári számát, típusát, valamint a benne lévő adathordozók törléséről szóló nyilatkozatot, a felelős munkatárs aláírásával.
d) A kényes információk kiszivárgásának megelőzése érdekében a selejtezendő adathordozókat a Főiskola munkatársai megsemmisítik. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

(5) Mentések, fájlok védelme
a) Az adatfeldolgozás után biztosítani kell az adatok mentését.
b) A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése és a mentés biztonságos tárolása az azt létrehozó felhasználók feladata.
c) A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok nyújtanak segítséget.
d) A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazdák a felelősek.

(6) Szoftvervédelem
a) Rendszerszoftver-védelem
A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.
b) Felhasználói programok védelme
a. Programhoz való hozzáférés, programvédelem:
i. A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.
ii. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.
b. Programok megőrzése, nyilvántartása:
i. A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetniük.
ii. A számvitelről szóló 2000. évi C. törvény 169. § értelmében az AVKF-nek az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 8 évig meg kell őriznie.
iii. 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.
iv. A programok nyilvántartásáért és működőképes állapotban való tartásáért az egységvezetők a felelősek.

20. § A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

(1) Szerverek
a) Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.
b) A szerverek háttértárairól folyamatosan biztonsági mentést kell készíteni.

c) Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.
d) A vásárolt szoftverekről biztonsági másolatot kell készíteni.

(2) Munkaállomások
a) A külső helyről hozott vagy kapott anyagokat vírusellenőrző programmal ellenőrizni kell.
b) Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
c) Az új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal kell ellenőrizni működésüket.
d) Az AVKF informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítése célján kívüli egyéb okból tilos.
e) A hálózati vezeték és egyéb csatlakozó elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
f) Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.
g) Az AVKF zárt hálózatára hálózati eszközt csak az informatikai vezető engedélyével szabad csatlakoztatni. Az engedély nélkül csatlakoztatott eszköz hálózati hozzáférését az észlelést követően azonnal meg kell szüntetni, az eszközt csatlakoztató személy ellen felelősségre vonási eljárást kell lefolytatni.

21. § Ellenőrzés

(1) Az ellenőrzési folyamatok célja, hogy elősegítse az informatikai rendszereknél előforduló veszélyhelyzetek kialakulásának megelőzését. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az ismét bekövetkezzen.

(2) Az IBSZ rendelkezéseit a Főiskola munkatársai és hallgatói betartani kötelesek.

22. § Felhasználói biztonsági rendelkezések

(1) Az AVKF munkatársainak munkavégzéséhez szükséges számítástechnikai eszközök a Főiskola tulajdonát képezik, azokat kizárólag munkavégzés céljára lehet használni.

(2) Eszközökkel kapcsolatos szabályok
a) Amennyiben a felhasználó bármilyen biztonsági problémát vagy hibát észlel, azonnal köteles értesíteni a rendszergazdát.
b) Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.
c) Tilos az eszközök közelében enni, inni, dohányozni.

(3) Jelszókezeléssel kapcsolatos szabályok
a) A munkavállaló felhasználó köteles jelszót beállítani. A jelszó minimum nyolc karakter hosszú, kis- és nagybetűket, valamint számokat is kell, hogy tartalmazzon.
b) A felhasználó köteles bizonyos időközönként (legalább 3 havonta) jelszavait lecserélni.
c) A jelszó jól látható vagy könnyen hozzáférhető helyre történő felírása tilos.
d) Tilos a névre szóló jelszó kiadása más felhasználók számára.

(4) Szoftverekkel kapcsolatos szabályok
a) A főiskola kizárólag jogtiszta szoftverekkel dolgozik.
b) A jogtisztaság biztosítása érdekében tilos az informatikusokon kívül bármely más felhasználónak bármilyen terjesztési engedéllyel (freeware, shareware, cardware, donateware, trial stb.) rendelkező szoftvert a főiskola tulajdonát

képező számítógépre feltelepíteni. A szoftverek törlését is csak az iskola informatikusai végezhetik el.

(5) Adatvédelmi szabályok
   a) A személyes, munkához közvetlenül nem kapcsolódó állományok tárolása mind a munkaállomásokon, mind a szervereken tiltott.
   b) Az AVKF működése során az AVKF e feladattal megbízott szakembere által készített kép-, hang-, valamint videofelvételek a főiskola tulajdonát képezik. Ezen anyagoknak engedély nélküli felhasználása, sokszorosítása tilos.

(6) Internethasználattal kapcsolatos szabályok
   a) Távoli hozzáféréshez kizárólag olyan szoftverek használhatók, amelyek kapcsolódás előtt kérik a felhasználó engedélyét a kapcsolat létesítéséhez.
   b) Tilos a munkahelyi internetkapcsolaton keresztül minden olyan program és egyéb fájl letöltése, amely nem a munkavégzéshez szükséges.
   c) A főiskola hálózatán és számítástechnikai eszközein nem engedélyezett semmilyen fájlmegosztó alkalmazás (DC++, BitTorrent) használata.

(7) Vírusvédelmi szabályok
   a) A számítógépeken vírusirtó program fut, mely a gép működése közben automatikusan figyeli a rendszert. A vírusirtó programot leállítani és annak működésébe beavatkozni szigorúan tilos.
   b) Minden fájlművelet előtt ez a program ellenőrzi a megnyitott fájlokat. Bármilyen, adatbiztonságot veszélyeztető esemény figyelmeztetése jelenik is meg a felhasználó monitorán, azonnal értesítenie kell a rendszergazdát, hogy ő a megfelelő lépésekkel megakadályozhassa a kártékony programok további fertőzéseit.
   c) Vírustalálat esetében a munkát azonnali hatállyal fel kell függeszteni, a számítógépet a belső hálózatról le kell választani és megkezdeni a helyreállítást, valamint az okok feltárását.

(8) Honlapkezelési szabályok

Az AVKF honlapjához kapcsolódó szabályokról a Kommunikációs szabályzat rendelkezik.

23. § Záró és átmeneti rendelkezések

(1) Az Informatikai biztonsági szabályzat új jogszabályok megjelenésével, valamint a jogszabályi módosításokkal összefüggő korrekciójáról a gazdasági igazgató gondoskodik, a korrekcióra vonatkozó javaslatot a szenátus elé terjeszti.

(2) A szabályzatot a szenátus 2025.06.12-i ülésén az SZH 72/2025.VI.12. számú határozatával fogadta el.

(3) Jelen szabályzat 2025.06.13-án lép hatályba.

Vác, 2025.06.12.

Dr. Gloviczki Zoltán
rektor