Ikt. sz.: RH/126/2019

10033832

Informatikai Biztonsági Szabályzata

(IBSZ)

APOR VILMOS

AVKF

KATOLIKUS FŐISKOLA

2019. augusztus

Tartalomjegyzék

1. A szabályzat célja ... 2
2. A szabályzat hatálya ... 3
3. Értelmező rendelkezések ... 3
4. Az IBSZ biztonsági fokozata ... 5
5. Kapcsolódó szabályzatok ... 5
6. Védelmet igénylő, az informatikai rendszerre ható elemek ... 5
7. A védelem tárgya ... 6
8. A védelem eszközei ... 6
9. A védelem felelőse ... 6
10. Az informatikai biztonsági felelősök és a felhasználók feladatai ... 7
11. Az informatikai vezető ellenőrzéssel kapcsolatos feladatai ... 8
12. Az informatikai vezető jogai ... 8
13. Az IBSZ megismerhetőségének és alkalmazásának módja ... 8
14. Az IBSZ felülvizsgálata ... 8
15. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság ... 9
16. Hozzáférési jogosultságok ... 9
17. Az informatikai eszközbázist veszélyeztető helyzetek ... 9
18. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek ... 11
19. Az informatikai eszközök környezetének védelme ... 12
20. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek ... 12
21. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága ... 15
22. Ellenőrzés ... 15
23. Felhasználói biztonsági szabályzat ... 16
24. Záradék ... 17

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 I. törvény 5/A pontja alapján a következő szabályzatot alkotja:

1. A szabályzat célja

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.

Az IBSZ célja továbbá:

a) az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
b) az üzemeltetett számítógépek, informatikai eszközök, valamint a kamera- és a beléptető rendszer 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
   a. Kiterjed az AVKF tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációjára is;
   b. a rendszer- és felhasználói programokra;
   c. a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
   d. az adatok felhasználására, tárolására vonatkozó utasításokra;
   e. az adathordozók tárolására, felhasználására;

3. Értelmező rendelkezések

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.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

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.

Adatkezelő: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.

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.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Információ: jelentéssel bíró adat, megjelenési módjára vagy formájára való tekintet nélkül.

Informatikai rendszer: a főiskola számítógép-hálózata, beleértve hálózati eszközöket, szervereket, általános célú számítógépeket, laptopokat, projektorokat, felhasználói és rendszerszoftvereket, sokszorosító, digitalizáló berendezéseket és a telefonrendszert.

Rendszergazda: az a számítástechnikai ismeretekkel rendelkező személy, akit ezzel a feladattal a felhatalmazott szervezeti egység vezetője írásban megbíz.
A rendszergazda a számítógép hardver és szoftver karbantartását, fejlesztését, hibáinak feltárását és – ha lehetséges – javítását végzi.

4. Az IBSZ biztonsági fokozata

Az IBSZ biztonsági fokozata az AVKF-nél alap biztonsági 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.)

Az AVKF általános informatikai feldolgozást végez.

5. Kapcsolódó szabályzatok

Az IBSZ előírásai összhangban vannak a:

a) Szervezeti és Működési Szabályzattal,
b) Leltározási és Leltárkészítési Szabályzattal,
c) Felesleges Vagyontárgyak Hasznosítási és Selejtezési Szabályzatával,
d) Belső Ellenőrzési Kézikönyvvel / Szabályzattal,
e) Kommunikációs Szabályzattal,
f) Tűzvédelmi Szabályzattal,
g) az Adatvédelmi és adatbiztonsági szabályzattal.

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.
Az informatikai rendszerre az alábbi tényezők hatnak:

a) a környezeti infrastruktúra,
b) a hardver elemek,
c) az adathordozók,
d) a dokumentumok,
e) a szoftver elemek,
f) az adatok,
g) a rendszerelemekkel kapcsolatba kerülő személyek.

7. A védelem tárgya

A védelmi intézkedések kiterjednek:

a) a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
b) az alkalmazott hardver eszközökre 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 a feldolgozást támogató rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználására, 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. A védelem felelőse

A védelem felelősei a mindenkori informatikai vezetők.

10. 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) a felhasználók számítógépén ellenőrzi a szoftverek használatának jogszerűségét,
   g) 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 hardver eszközeinek karbantartásáért,
   f) nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
   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.

3) A felhasználó feladatai
   a) az általa létrehozott adatok mentésének biztosítása,
   b) hozzáférési azonosítóinak és a hozzájuk tartozó jelszavai titkosságának megőrzése.

11. 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.

12. Az informatikai vezető jogai

1) Az előírások be nem tartása esetén felelősségre vonási eljárást kezdeményezhet a Rektornál,
2) bármely érintett szervezeti egységnél jogosult ellenőrzésre,
3) betekinthet az informatikai feldolgozásokkal kapcsolatos valamennyi iratba,
4) javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
5) adatvédelmi és adatbiztonsági szempontból véleményezi az informatikai beruházásokat.

13. Az IBSZ megismerhetőségének és alkalmazásának módja

1) Az IBSZ megismerését az érintett dolgozók részére a vezetők és a rendszergazdák a főiskola honlapján való közzététel formájában biztosítják.
2) Az IBSZ által érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

14. 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.

15. 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) Az informatikai feldolgozás során keletkező adatok minősítője a főiskola felsővezetése.
3) A különös védelmi utasításoknak és szabályozásoknak összhangban kell lenniük a hatályos jogszabályokkal.
4) A titokvédelmi szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát az érintett alkalmazottakkal ismertetni kell.
5) Mindenki csak ahhoz az adathoz férhet hozzá, amelyre a munkájához feltétlen szüksége van.
6) 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.
7) A naplófájlokat rendszeresen át kell tekinteni, és a jogosulatlan hozzáférést vagy annak a kísérletét a szervezeti egység vezetőjének azonnal jelenteni kell.
8) A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.
9) A titkot képező adatok védelmét az adatfeldolgozás, adattovábbítás, adattárolás során az operációs rendszerben és a felhasználói programban alkalmazott logikai, matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

16. Hozzáférési jogosultságok

Az informatikai rendszerekhez hozzáférési jogosultságot igényelni, vagy jogosultság változást kérni az informatikai vezetőtől az it@avkf.hu email címen lehet.
A hozzáférési jogosultsági igényt az igénylő személy szervezeti egységének vezetője és az AVKF rektora bírálja el, jóváhagyása szükségszerű.
A beérkezett és elbírált hozzáférési jogosultságok kiosztását, illetve módosítását az Oktatástechnika erre a feladatra feljogosított munkatársai végzik.

17. 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.

1) Környezeti infrastruktúra okozta ártalmak

a) Elemi csapás:
- földrengés
- árvíz
- tűz
- villámcsapás, egyéb vis major

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

c) Közüzemi szolgáltatásban bekövetkező zavarok
- feszültség-kimaradás
- feszültségingadozás
- elektromos zárlat
- csőtörés

2) Emberi tényezőre visszavezethető veszélyek

a) 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, hálózati forgalom)

b) 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

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.

18. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

1) A tervezés és az előkészítés során előforduló veszélyforrások
- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

2) A rendszerek megvalósítása során előforduló veszélyforrások
- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

3) A működés és fejlesztés során előforduló veszélyforrások
- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

19. 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 azonnal jelenteni kell,
e) az informatikai eszközöket csak a főiskola alkalmazottjai, ill. a hallgatói jogviszonnyal rendelkező diákok használhatják,
f) az informatikai eszközök rendeltetésszerű használatáért a felhasználó 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 kell vissza is helyezni
c) az Oktatástechnika adathordozói kivételével a bizalmas, valamint titkos adatokat tartalmazó eszközöket a főiskola irattárában, a többi anyagoktól elkülönítve, zárt helyen kell tárolni
d) a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek
e) adathordozót más szervezetnek átadni csak az egységvezető, vagy az informatikai vezető engedélyével szabad
f) a munkák befejeztével a használt berendezést az eredeti tárolási helyre vissza kell tenni

3) Elektronikus adattovábbítás

a) Az AVKF hálózatára csak hálózati azonosító birtokában szabad csatlakozni,
b) a hálózati azonosítókat, digitális aláírásokat központilag az Oktatástechnika kezeli, és tartja nyilván,
c) hivatalos dokumentumot interneten közzétenni, harmadik fél felé továbbítani csak nem szerkeszthető formátumban, a megfelelő engedélyeztetési eljárás megtörténte után szabad.

4) Tűzvédelem

A hatályos tűzvédelmi szabályzat szerint.

20. 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 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) Hardver védelem

a) A berendezések hibátlan és üzemszerű működését biztosítani kell.
b) A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
c) Az üzemeltetési, karbantartási és szervizelési feladatok ellátásáról az Oktatástechnika gondoskodik.
d) A javítási munkák elvégzésekor figyelembe kell venni:
   - a gyártó előírásait, ajánlatait,
   - a tapasztalatokat.
e) Bármely számítógép, vagy számítástechnikai eszköz szétbontását csak az Oktatástechnika beosztottja, vagy az informatikai vezető által kijelölt személy végezheti el. (Garanciális eszközök esetén a garanciális javítást végző szerviz munkatársa.)

3) Az informatikai feldolgozás folyamatának védelme

A) Az adatrögzítés védelme

a) adatbevitel hibátlan műszaki állapotú berendezésen történjen,
b) csak tesztelt adathordozóra lehet adatállományt rögzíteni,
c) a bizonylatokat és adathordozókat csak az e célra kialakított és megfelelő tároló helyeken szabad tartani,
d) az adatrögzítés szoftver védelme. Lehetőség szerint olyan szoftvereket kell vásárolni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
e) hozzáférési lehetőség:
   e)a) a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egység vezetője által kijelölt személyek férjenek hozzá);
   e)b) az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti;
   e)c) a szerverek rendszergazda jelszavát az informatikai vezető kezeli, és másolatban a rektor részére átadja.

B) Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

C) Az adathordozók megőrzése

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.

D) 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 alkatrész gyári számát, típusát, valamint a benne lévő adathordozók törléséről szóló nyilatkozatot, a felelős munkatárs aláírásával.

d) A kényes információk kiszivárgásának megelőzése érdekében a selejtezendő adathordozók esetében a sikeres törlés tényét ellenőrizni kell. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

E) Leltározás

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

F) Mentések, file-ok 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 munkatársak (felhasználók) feladata.

c) A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.

d) A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazdák a felelősek.

G) Szoftver védelem

a) Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

b) Felhasználói programok védelme

b)a) Programhoz való hozzáférés, programvédelem:

b)a)a) A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

b)a)b) Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

b)b) Programok megőrzése, nyilvántartása:

*b)b)a)*A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni az IBSZ 1. számú melléklete szerint.

b)b)b) 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 őrizni.

b)b)c) 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.

b)b)d) A programok nyilvántartásáért és működőképes állapotban való tartásáért az egységvezetők a felelősek.

21. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

1) Szerverek

a) Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültség-ingadozásoktól, 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 ellenőrizni kell vírusellenőrző programmal.

b) Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

c) 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 kielégítésein kívül tilos.

e) A hálózati vezeték és egyéb csatoló 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 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 ezen szabályzat 12. 1) pontja alapján az eljárást le kell folytatni.

22. Ellenőrzés

1) Az AVKF éves belső ellenőrzési tervében rögzíti az ellenőrzés módját.

2) 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 ismét bekövetkezzen.

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

23. Felhasználói biztonsági rendelkezések

Az AVKF a dolgozók munkavégzéséhez szükséges számítástechnikai hátteret biztosítja, a biztosított eszközöket azonban kizárólag munkavégzés céljára lehet használni. A biztosított eszközök a főiskola tulajdonát képezik.

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

2) Jelszókezeléssel kapcsolatos szabályok
   a) A felhasználó időközönként (javasolt legalább 3 havonta) köteles jelszavait lecserélni.
   b) A jelszó minimum nyolc karakter hosszú, kis- és nagybetűket, valamint számokat is kell, hogy tartalmazzon.
   c) A jelszó nem írható le semmilyen jól látható, vagy könnyen hozzáférhető helyre.
   d) Tilos a névre szóló jelszó kiadása más felhasználók számára.

3) 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.

4) Adatvédelmi szabályok
   a) A személyes, munkához közvetlenül nem kapcsolódó állományok tárolása mind a munkaállomásokon, mind a szervereken tiltott.
   b) A számítógépen tilos mappa megosztást kezdeményezni, azt fenntartani.
   c) 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. A multimédiás anyagok adathordozókra rögzített példányainak hozzáférhetőségéről, tárolásáról jelen szabályzat 20. 3) pontja rendelkezik.

5) Internethasználattal kapcsolatos szabályok

a) Tilos a munkahelyen minden – nem a napi munkával összeegyeztethetően használt – valós idejű kommunikációs program használata. Ide tartozik a Skype, ICQ, IRC, Viber és egyéb hasonló üzenetküldő használata. Tilos továbbá WEB- felületen keresztül elérhető valós idejű üzenetküldő úgynevezett "chat" program használata.

b) Tiltott a távoli számítógép-vezérlést és fájl-átvitelt biztosító szoftverek (pl. TeamViewer, LogMeIn) nem munkavégzés céljára való használata.
Indokolt esetben az Oktatástechnika jogosult központilag tiltani ezen alkalmazásokhoz szükséges feltételeket.

c) Tilos a munkahelyi Internet kapcsolaton keresztül minden olyan program és egyéb fájl letöltése, ami nem a munkavégzéshez szükséges.

d) Tilos minden Internetes "online" sugárzott műsor (ide tartoznak a rádió, televízió műsorok) hallgatása, megtekintése az Internet sávszélesség indokolatlan használata miatt. Az informatikai vezető, valamint a rendszergazdák jogosultak az Internet kapcsolat sávszélességének és forgalmának ellenőrzésére, korlátozására, amennyiben azt valamilyen konkrét észrevétel indokolja.

e) Mindenféle fájlmegosztó alkalmazás (DC++, BitTorrent, stb.) használata a főiskola számítástechnikai eszközein, valamint hálózatán tiltott.

6) 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 az adathálózatról le kell választani és megkezdeni az okok feltárását és a helyreállítást.

7) Honlapkezelési szabályok

Az AVKF honlapjához kapcsolódó szabályokról a Kommunikációs Szabályzat rendelkezik.

24. Záradék

Jelen szabályzatot az Apor Vilmos Katolikus Főiskola Szenátusa az **SZH 2019.08.29./50.** számú határozatával, 2019. szeptember 1-jei hatállyal fogadta el.

Vác, 2019. szeptember 4.

.....

Libor Józsefné dr.

rektor

Apor Vilmos Katolikus Főiskola AVKF Rektor

SZOFTVER NYILVÁNTARTÁS

Szoftver neve: .....
Szoftver gyártója: .....
Leltárszám: .....
Szoftver verziószáma: .....
Szoftver leírása: .....
.....
.....
Szoftver azonosító sorszáma, szériaszáma: .....
Szükséges hardver környezet: .....
.....
Szükséges operációs rendszer, szoftverkörnyezet: .....
.....
Licenc feltételei (kik, hányan, hány számítógépen, mettől-meddig használhatják): .....
.....
Szoftver típusa (OEM, frissítés): .....
.....
Darabszám: .....
Egyéb: .....
.....
.....

Adatfelvétel időpontja: .....

.....
Adatfelvevő aláírása