Elektronikusan aláírta:
Varga Andrea
Szigró

NYÍREGYHÁZI VIZSGAKÖZPONT
4400 Nyíregyháza, Árok utca 53.
Tel: +36 70-705-0957
E-mail cím: vizsgakozpont@nyiregyhaziavk.hu

Nyíregyházi Vizsgaközpont

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

11.verzió

Érvénybe lép: 2026.06.22.

Kiadta:

Varga Andrea
vizsgaközpont vezető

ZÁRADÉK: A dokumentum digitális aláírással hitelesített.

NYÍREGYHÁZI VIZSGAKÖZPONT
4400 Nyíregyháza, Árok utca 53.
Tel: +36 70-705-0957
E-mail cím: vizsgakozpont@nyiregyhaziavk.hu

Módosítások jegyzéke		
Fejezet	Utolsó módosítások tartalma	Módosítás dátuma
	Fejlécmódosítás	2022.03.31.
	Fejléc módosítás – székhelyváltozás	2022.09.19.
	Fejléc módosítása- logó	2023.02.01.
teljes dokumentum	felülvizsgálat	2024.02.22.
teljes dokumentum	A szakképzési törvény és annak végrehajtási rendeletének változása miatt	2024.07.01.
oldalszámozás	oldalszám/összes oldal száma	2024.11.04.
teljes dokumentum	lábléc módosítása	2025.01.06.
6.1	ellenőrizheti	2025.05.05.
7.	Az IBSZ megismerését az érintett dolgozók részére a vizsgaközpont biztosítja.	2025.05.05.
fedlap	Vizsgaközpont vezető váltás	2026.06.22.

Tartalom

1. Az Informatikai Biztonsági Szabályzat célja 5
2. Az Informatikai Biztonsági Szabályzat hatálya 6
2.1. Személyi hatálya 6
2.2. Tárgyi hatálya 6
3. Az adatkezelés során használt fontosabb fogalmak 6
4. Az IBSZ biztonsági fokozata 7
5. Védelmet igénylő, az informatikai rendszerre ható elemek 7
5.1. A védelem tárgya 8
5.2. A védelem eszközei 8
6. A védelem felelőse, vezetői 9
6.1. A Vizsgaközpont adatvédelmi tisztviselőjének ellenőri feladatai 10
6.2. A Vizsgaközpont adatvédelmi tisztviselőjének jogai 10
7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja 11
7.1. Az Informatikai Biztonsági Szabályzat karbantartása 11
7.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság 11
8. Az informatikai eszközbázist veszélyeztető helyzetek 12
8.1. Környezeti infrastruktúra okozta ártalmak 12
8.2. Emberi tényezőre visszavezethető veszélyek 13
9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek 13
9.1. Tervezés és előkészítés során előforduló veszélyforrások 13
9.2. A rendszerek megvalósítása során előforduló veszélyforrások 13
9.3. A működés és fejlesztés során előforduló veszélyforrások 14
10. Az informatikai eszközök környezetének védelme 14
10.1. Vagyonvédelmi előírások 14
10.2. Adathordozók 14
10.3. Tűzvédelem 14
10.4. Elektronikus levelezés szabályai 15

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek 15
11.1. A számítógépek és szerverek védelme 15
11.2. Hardver védelem 15
11.3. Az informatikai feldolgozás folyamatának védelme 16
11.3.1. Az adatrögzítés védelme 16
11.3.2. Az adathordozók nyilvántartása 16
11.3.3. Adathordozók tárolása 16
11.3.4. Az adathordozók megőrzése 16
11.3.5. Selejtezés, sokszorosítás, másolás 17
11.3.6. Leltározás 17
11.3.7. Mentések, file-ok védelme 17
11.4. Szoftver védelem 17
11.4.1. Rendszerszoftver védelem 17
11.4.2. Jelszavak hozzáférésének kezelése, tárolása 17
11.4.3. Felhasználói programok védelme, programokhoz való hozzáférés, programvédelem 18
11.4.4. Programok megőrzése, nyilvántartása 18
12. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága 18
12.1. Központi gépek 18
12.2. Munkaállomások 18
13. Ellenőrzés 19

A Nyíregyházi Vizsgaközpont (a továbbiakban: Vizsgaközpont) az Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés, valamit az Európai Parlament és a Tanács (EU) 2016. április 27. napján kiadott 2016/679 Rendelete (GDPR) (továbbiakban: Rendelet) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK Rendelet hatályon kívül helyezéséről szóló általános adatvédelmi rendelet alapján a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

A Vizsgaközpont IBSZ-nak alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ 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 üzembehelyezésen keresztül az üzemeltetésig.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem, és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed a Vizsgaközpont belső munkaszervezetére, annak valamennyi dolgozójára, illetve az informatikai eljárásban résztvevőkre.

2.2. Tárgyi hatálya

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

3. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik;

Adattovábbítás: az adat meghatározott harmadik fél számára történő hozzáférhetővé tétele.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja;

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

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.

4. Az IBSZ biztonsági fokozata

A Vizsgaközpont adatai különböző biztonsági fokozatba tartozhatnak (üzleti titkok, pénzügyi adatok), illetve a Vizsgaközpont belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok. Az adatokhoz való hozzáférés kizárólag a foglalkoztatott munkavégzéséhez szükséges adatokra vonatkozik, amelyre a munkaköri leírásban foglaltak az irányadóak.

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:

- az alkalmazott hardver eszközökre és azok működési biztonságára, valamint a tárolás helyéül szolgáló helyiségekre,
- 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 (pl. személyes adatok védelme) és vagyoni jogokra (pl. szerzői jogvédelem).

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.

Az informatikai eszközök egyedi jelszóval védettek, melyek kizárólag az gép használója ismer. A jelszavakat lezárt borítékban, páncélszekrényben tárolja a vizsgaközpont vezető, melyet indokolt esetben (pl: hosszan tartó betegség) felhasznál, ez esetben a jelszót meg kell változtatni és azt az őrzés helyére zárt borítékba elhelyezni.

A Vizsgaközpont informatikai rendszerét (vizsgajelentésre alkalmas rendszer) a fenntartó működteti, hozzáférési jogosultságot a rendszeren keresztül lehet igényelni a rendszer működtetője által

meghatározott feltételekkel. A jelszavakat a vizsgaközpont vezetője nyilvántartja, és elzárt helyen tárolja.

6. A védelem felelőse, vezetői

A védelem felelősei az adatvédelmi tisztviselő és a rendszergazda. Az adatvédelmi tisztviselő a Nyíregyházi Szakképzési Centrum által biztosított.
A jelen szabályzatban foglaltak szakszerű végrehajtásáról a vizsgaközpont vezetőjének kell gondoskodnia.

a) Adatvédelmi tisztviselő feladatai:

Az adatvédelmi tisztviselő a Vizsgaközpontban legalább a következő feladatokat ellátja:

- tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére,
- ellenőrzi a rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- együttműködik a felügyeleti hatósággal;
- az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- 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,

- nyilvántartja, nyilvántarttatja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- ellenőrzi a szoftverek használatának jogszerűségét.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

b) Rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a Vizsgaközpont informatikai rendszer hardver eszközeinek karbantartásáért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- gondoskodik a folyamatos vírusvédelemről,
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját.

6.1. A Vizsgaközpont adatvédelmi tisztviselőjének ellenőri feladatai

- részletesen ellenőrizheti az IBSZ előírásainak betartását,
- ellenőrizheti a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrizheti az informatikai munkafolyamat bármely részét.

6.2. A Vizsgaközpont adatvédelmi tisztviselőjének jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a vizsgaközpont vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,

- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vizsgaközpont biztosítja.

7.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint a Vizsgaközpontnál - bekövetkező jogi és technikai változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az adatvédelmi tisztviselő feladata, aki jelzi az IBSZ aktualizálásának szükségességét a vizsgaközpont vezetőjének.

7.2. 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 a vizsgaközpont vezetője.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi 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.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.

A naplófájlokat rendszeresen át kell tekinteni, és a jogosulatlan hozzáférést vagy annak a kísérletét a vizsgaközpont vezetőjének jelenteni kell. A vizsgaközpont vezetője dokumentáltan tájékoztatja a kancellárt és a főigazgatót.

A naplófájlok áttekintéséért, értékeléséért a rendszergazda a felelős.

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).

Minden dolgozóval (munkaviszony, megbízási szerződés, vagy bármilyen más jogviszony), aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut, titoktartási és pártatlansági nyilatkozatot kell aláíratni.

A nyilatkozatot a jogviszony kezdetekor kell aláíratni, és a megbízott dokumentumai között tárolni.

8. 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. A szabályzat megismeréséről, a megismerési nyilatkozat aláírásával a munkavállaló nyilatkozik.

8.1. 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.

8.2. 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 megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala a Centrum számítógépeire,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

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

- minden helyiséget ahol informatikai eszközök vannak, biztonsági zárakkal kell felszerelni,
- a helyiségekbe belépés csak az arra illetékeseknek engedélyezett,
- a helyiségekbe, szerverterembe történő illetéktelen behatolás tényét a vizsgaközpont vezetőnek azonnal jelenteni kell,
- az informatikai eszközöket csak a Vizsgaközpont arra felhatalmazott munkatársai használhatják,
- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

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, melyről nyilvántartást kell vezetni - tárgyi eszközök nyilvántartása (Centrum),
- 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.

10.3. Tűzvédelem

A szerverterem illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt kockázati osztályt jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
A szerverszobába minimum 1 db tűzoltó készüléket kell elhelyezni.
A szerverszobában elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

10.4. Elektronikus levelezés szabályai

Az e-mail (elektronikus levél) számítógépes hálózatokon keresztül továbbított levél, üzenet. Tartalma lehet szöveg, kép, hang, mozgókép.
A Vizsgaközpont belső munkaszervezetében dolgozóknak a Nyíregyházi Vizsgaközpont biztosít elektronikus levelezési címet. Az e-mail cím a dolgozó nevéből képzett levelezési cím. Az e-mail cím általános alakja: Név (a felhasználó nevéből képzett cím) + @ (kukac) + Kiszolgáló (a levelezőszerver címe). A dolgozók munkavégzés közben kizárólag a vizsgaközpont vezető által kiosztott e-mail címeket használhatják. Adatvédelmi szempontokra hivatkozva és az adatvédelmi szabályzatban foglaltakra tekintettel, a Vizsgaközpontban TILOS a magán e-mail címekről történő levelek továbbítása és fogadása.

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

11.1. 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:

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

11.2. Hardver védelem

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, ajánlatait,

- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

11.3. Az informatikai feldolgozás folyamatának védelme

11.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és adathordozókat csak az e célra kialakított és megfelelő tároló helyeken szabad tartani,

Az adatrögzítő szoftver védelme érdekében lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek:

- rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.

Hozzáférési lehetőség:

- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A szerverek rendszergazda jelszavát a rendszergazda kezeli.

11.3.2. Az adathordozók nyilvántartása

Az adathordozókról nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

11.3.3. Adathordozók tárolása

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

11.3.4. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylatőrzési kötelezettségnek megfelelően kell kialakítani, ennek szabályozása a Vizsgaközpont Dokumentum és iratkezelési szabályzatában található.

11.3.5. Selejtezés, sokszorosítás, másolás

A selejtezést a Centrum selejtezési szabályzata alapján kell lefolytatni. A selejtezést a Centrum irányítja. Sokszorosítást, másolást csak belső utasítás szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

A másolt adatok csak a vizsgaközpont vezető engedélyével adhatók ki.

11.3.6. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

11.3.7. Mentések, file-ok védelme

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. Az archiválásban a rendszergazda segítséget nyújt. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért a rendszergazda a felelős.

11.4. Szoftver védelem

11.4.1. Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

11.4.2. Jelszavak hozzáférésének kezelése, tárolása

A vizsgaközpont vezetője és munkatársai részére kiosztott felhasználó neveket és jelszavakat a vizsgaközpont vezetőjének irodájában elhelyezett páncélszekrényben, zárt borítékban tárolja. A felhasználói nevekhez és jelszavakhoz történő hozzáférést a vizsgaközpont vezető engedélyezheti irányítási területüknek megfelelően. Az egyes felhasználókhoz adott hozzáféréseket a felhasználóknak egyénileg titkosan kell kezelnie, ez az adott felhasználó névhez és jelszóhoz rendelt felhasználó feladata és felelőssége.

Elvesztett, elfelejtett felhasználó név és jelszó esetén a vizsgaközpont vezetőt kell értesíteni, aki gondoskodik a jelszó érvénytelenítéséről vagy új jelszó kiadásáról. A jelszavakat változás esetén, a páncélszekrényben is ki kell cserélni, hogy minden alkalommal az érvényes jelszó kerüljön tárolásra.

11.4.3. Felhasználói programok védelme, programokhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Minden felhasználónak jelszóval kell védenie a programját. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell. A jelszót nem szabad több személy között megosztani. A felhasználók jelszavát a felhasználón kívül senki sem ismerheti. A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott. A jelszavak alkalmazását, időszakos módosítását a rendszergazda szúrópróbaszerűen ellenőrzi. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

11.4.4. Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni. (nyilvántartás: Centrum)
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.

12. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

12.1. Központi gépek

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.

12.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket. A Vizsgaközpont 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 csak az eszköz leltárfelelőse és a rendszergazda tudtával és engedélyével szabad.

13. Ellenőrzés

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.