# DEBRECENI EGYETEM
# NÉPEGÉSZSÉGÜGYI KAR

# INFORMATIKAI SZABÁLYZAT

**Debrecen,**
**2014. november 10.**

## Tartalom

# 1. Az Informatikai Szabályzat célja

A 21. században minden eddigi kort meghaladó gyorsasággal és mennyiségben keletkeznek új információk. Az információk keletkezésének, kezelésének, kibocsátásának és felhasználásának központi szereplői a felsőoktatási intézmények, melyek ez által aktív résztvevői egy információs, tudás alapú társadalomnak.
A Debreceni Egyetem Népegészségügyi Kar (DE NK) informatikai rendszere az európai színvonalnak megfelelő, garantált minőségű, ellenőrzött hozzáférésen keresztül a magyar felsőoktatásban alkalmazott minőségi szolgáltatásokat nyújtja, és biztosítja az információs társadalom eszközeihez való hozzáférést az oktatók, a kutatók, az alkalmazottak és a hallgatók számára azzal a céllal hogy munkájukban éstanulmányaikban a lehető legoptimálisabb teljesítményt nyújtsák
Az informatikai szolgáltatásokhoz való hozzáférés szükséges feltételeit és szabályait az Informatikai Szabályzat (ISZ) tartalmazza.
Az ISZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az ISZ 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 üzembe helyezésen keresztül az üzemeltetésig.
A jelen ISZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

# 2. Az Informatikai Szabályzat hatálya

### *2.1. Felhasználók*

Jelen szabályzat hatálya kiterjed valamennyi felhasználóra, aki a Debreceni Egyetem Népegészségügyi Kar, alkalmazottjaként, hallgatójaként vagy a Debreceni Egyetem Népegészségügyi Kar területén tartózkodó vendégként, egyéb jogcímen feljogosítottként a Kar informatikai rendszerének eszközeit és szolgáltatásait rendszeresen vagy alkalmanként igénybe veszi (a továbbiakban: felhasználó)

.

A Debreceni Egyetem Népegészségügyi Kar minden alkalmazottja és hallgatója addig jogosult a Kar informatikai hálózatának szolgáltatásait igénybe venni, amíg az intézménnyel munkaviszonyban, alkalmazotti viszonyban vagy hallgatói jogviszonyban (a továbbiakban: jogviszony) áll.

A jogviszony megszüntetése előtt a Kar informatikai vezetője intézkedik a felhasználó egyetemi szervereken lévő azonosítóinak és az azokhoz kapott tárterületek, valamint az intézményi e-mail címeinek, a NEPTUN rendszerhez és az e-Learning keretrendszerhez kiadott hozzáférési jogosultságainak megszüntetéséről, archiválásáról.

### *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 Debreceni Egyetem Népegészségügyi Kar tulajdonában 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 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;

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

***Adattovábbítás:*** ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

***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.

***Adatfeldolgozó:*** az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

***Nyilvánosságra hozatal:*** ha az adatot bárki számára hozzáférhetővé teszik;

***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 Informatikai Szabályzat biztonsági fokozata

A Debreceni Egyetem Népegészségügyi Kar adatai különböző biztonsági fokozatba tartozhatnak. (közszolgálati titkok, pénzügyi adatok, illetve az Egyetem, illetve a Kar belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

## 5. Kapcsolódó szabályozások

Az ISZ előírásai összhangban vannak:

- Leltározási és értékelési szabályzattal,
- Számviteli szabályozással

# 6. 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.

## *6.1. A védelem tárgya*

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.

## *6.2. 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.

# 7. A védelem felelőse

**A védelem felelőse a mindenkori informatikai vezető.**
A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Debreceni Egyetem Népegészségügyi Kar dékánjának kell gondoskodnia.

### *7.1. Adatvédelmi felelősök feladatai*

a) Informatikai vezető feladatai:
– az ISZ 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, ismertetése,
– ellenőrzi a szoftverek használatának jogszerűségét
– gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
– felelős a Debreceni Egyetem Népegészségügyi Kar informatikai rendszer hardver eszközeinek karbantartásáért,
– nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
– folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
– ellenőrzi a rendszer adminisztrációját.

b) Informatikus feladatai:
– az informatikus (rendszergazda) az informatikai vezető által a saját feladatkörébe utalt rendszert felügyeli,
– felelős az általa kezelt informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
– gondoskodik a folyamatos vírusvédelemről
– a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről.

### *7.2. Az informatikai vezető ellenőri feladatai*

– évente egy alkalommal részletesen ellenőrzi az ISZ előírásainak betartását,
– rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
– előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

### *7.3. Az informatikai vezető jogai*

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Debreceni Egyetem Népegészségügyi Kar dékánjánál, illetve intézet/tanszék 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.

# 8. Az Informatikai Szabályzat alkalmazásának módja

Az ISZ megismerését az érintett dolgozók részére a vezetők és az informatikai szakemberek oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
Az Informatikai Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az ISZ előírásainak megfelelően.

## *8.1. Az Informatikai Szabályzat karbantartása*

***Az ISZ-ot az informatikában - valamint a Karnál - bekövetkező változások miatt időközönként aktualizálni kell. Az ISZ folyamatos karbantartása az informatikai vezető feladata.8.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság***

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:
– közlésre szánt, bárki által megismerhető adatok,
– minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.
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 vagy mágneslemezre 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 Népegészségügyi Kar dékánjának, illetve az intézet vezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák 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).

## 9. 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.

### *9.1. Környezeti infrastruktúra okozta ártalmak*

elemi csapás:

- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.

környezeti kár:

- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának emelkedése vagy csökkenése,
- szennyeződés (pl. por).

közüzemi szolgáltatásba bekövetkező zavarok:

- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

### *9.2. 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,
- 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.

## 10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

### *10.1. Tervezés és előkészítés során előforduló veszélyforrások*

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

### *10.2. A rendszerek megvalósítása során előforduló veszélyforrások*

– hibás adatállomány működése,
– helytelen adatkezelés,
– programtesztelés elhagyása.

### *10.3. A működés és fejlesztés során előforduló veszélyforrások*

– emberi gondatlanság,
– szervezetlenség,
– képzetlenség,
– szándékosan elkövetett illetéktelen beavatkozás,
– illetéktelen hozzáférés,
– üzemeltetési dokumentáció hiánya.

# 11. Az informatikai eszközök környezetének védelme

### *11.1. Vagyonvédelmi előírások*

– a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
– a gépterembe való be- és kilépés rendjét szabályozni kell,
– a gépterembe, szerver terembe történő illetéktelen behatolás tényét az Népegészségügyi Kar dékánjának azonnal jelenteni kell,
– az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

### *11.2. 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,
– a használni kívánt adathordozót (pl. CD, DVD) 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,

### *11.3. Tűzvédelem*

A gépterem illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
A Kar géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.
A Kar géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.
A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

# 12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

### *12.1. 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.

### *12.2. 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 a megbízott informatikus végezheti el.

### *12.3. Az informatikai feldolgozás folyamatának védelme*

#### *12.3.1. Az adatrögzítés védelme*

– adatbevitel hibátlan műszaki állapotú berendezésen történjen,
– tesztelt adathordozóra lehet adatállományt rögzíteni,
– a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
– az adatrögzítő szoftver védelme. 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 az informatikai vezető kezeli.
  Az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,

- ellenőrző rögzítési utasítások,
- tesztelő és törlő programok kezelési utasításai,
- megőrzési utasítások,
- gépkezelési leírások.

### *12.3.2. Az adathordozók nyilvántartása*

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

### *12.3.3. Adathordozók tárolása*

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

### *12.3.4. Az adathordozók megőrzése*

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

### *12.3.5. Selejtezés, sokszorosítás, másolás*

A selejtezést a Debreceni Egyetemselejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

### *12.3.6. Leltározás*

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

### *12.3.7. 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.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

### *12.4. Szoftver védelem*

#### *12.4.1. Rendszerszoftver védelem*

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

#### *12.4.2. Felhasználói programok védelme*

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

**Programok megőrzése, nyilvántartása**

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni
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.

## 13. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

### *13.1. 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.
A vásárolt szoftverekről biztonsági másolatot kell készíteni.

### *13.2. Munkaállomások*

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 Debreceni Egyetem Népegészségügyi Kar 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 tudtával és engedélyével szabad.

## 14. 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.
A munkafolyamatba épített ellenőrzés során az ISZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

## 15. Informatikai szolgáltatások igénylése

A szolgáltatások igénylésének, és regisztrálásának köre kiterjed a DE Népegészségügyi Kar összes intézetére és tanszékére.

### *15.1. A DE ISZK-tól igényelhető szolgáltatások:*

- hálózati azonosító igénylése, vagy megváltoztatása,
- új e-mail cím, vagy meglévő módosításának igénylése,
- NEPTUN hozzáférés módosításának igénylése (a tanulmányi osztályvezetővel együttműködve),
- e-Learning rendszerhez fejlesztőként való hozzáférés igénylése,
- egyetemi szoftver liszensz igénylése (pl. SPSS, EndNote, SAS),
- WEB tárhely igénylése,
- domain név igénylése (egyetemi tartományba unideb.hu, unideb.com alá),
- VPN szolgáltatás igénylése.

***15.2. A szolgáltatás igénylésének, megszüntetésének menete:***

- A szolgáltatásokat a Népegészségügyi Kar mindenkori informatikai vezetője engedélyezi, vagy igényli meg a DE ISZK-tól.
- Ettől csak a távollétében és sürgős esetben lehet eltérni, de erről az informatikai vezetőt írásban, lehetőleg e-mailben értesíteni kell.
- a dolgozói jogviszony megszüntetése előtt a Kar informatikai vezetője intézkedik a felhasználó egyetemi szervereken lévő azonosítóinak és az azokhoz kapott hozzáférések, valamint az intézményi e-mail címeinek, a NEPTUN rendszerhez és az e-Learning keretrendszerhez kiadott hozzáférési jogosultságainak megszüntetéséről, archiválásáról.
- az igényelt egyetemi tárhelyek, domain nevek minden évben felmérésre kerülnek, és amennyiben már nincs igény a használatukra intézkedik a felszabadításukról, vagy megszüntetésükről.

## 16. Beszerzés, karbantartás, javítás

- A számítógépek és hálózatok beszerzésére, karbantartására, a mindenkor érvényben lévő, egyetemi gazdasági, logisztikai szabályozások érvényesek. Ezek menete a szabályzatokban aktualizálva van.
- A beszerzéseket, a Kar informatika vezetőjének ellenjegyeznie kell, hogy a fejlesztések illeszkedjenek a már meglévő géppark struktúrájába.
- Az információ technológiai eszközök karbantartása, javítása a kar mindenkori informatikai vezetővel történt egyeztetés után történhet meg, mérlegelve a ráfordítás és a használhatóság paramétereit.
- Az Kar informatikai vezetője, egyeztet, és jóváhagyatja a javításokat a Debreceni Egyetem informatikai vezetőjével.