KOCH RÓBERT KÓRHÁZ ÉS RENDELŐINTÉZET
BEL ÉS TÜDŐINTÉZET
A Debreceni Egyetem részjogú akkreditált szakorvos képző helye
3780 Edelény, Dankó Pista u. 80. Pf. 63.
Tel.: 48/524-040 Fax: 48/341-632 email: titkarsag@krkedeleny.hu

Iktatási szám: 54-13/2016

INFORMATIKA BIZTONSÁGI SZABÁLYZAT

Hatályba lépés napja: 2017. február 01.

	Név, beosztás	Dátum	Aláírás
Készítette:	Veres József főinformatikus	2016. 11. 20.	
Jóváhagyta:	Dr. Daher Pierre főigazgató	2016. 12.23.	

Nyilvántartott összes példány száma: 16
Jelen példány sorszáma: 1

TARTALOMJEGYZÉK

I. A JELEN SZABÁLYZAT CÉLJA

A jelen szabályzat alapvető **célja**, hogy az informatikai rendszer alkalmazása során biztosítsa az államháztartás szervezetének az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzat további céljai:

- a titok-, munka, 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 üzemeltetésükön keresztül a felhasználásig.

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

II. A JELEN SZABÁLYZAT HATÁLYA

A jelen szabályzat **személyi hatálya** az államháztartás szervezete valamennyi fő- és részfoglalkozású dolgozójára.

A szabályzat **tárgyi hatálya**

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül;
- kiterjed az államháztartás szervezete tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is;

- 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.

III. ALAPFOGALMAK

- **érintett:** bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;
- **személyes adat:** az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;
- **különleges adat:**a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;
- **közérdekű adat:** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;
- **közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;
- **adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;

- **adatkezelés:** az alkalmazott eljárástól függetlenül az adatokon 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 adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
- **adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- **nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;
- **adattörlés:** az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;
- **adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;
- **adatzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;
- **adatmegsemmisítés:** az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;
- **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 adatokon végzik;
- **adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi;
- **adatfelelős:** az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;
- **adatközlő:** az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;
- **adatállomány:** az egy nyilvántartásban kezelt adatok összessége;

IV. BIZTONSÁGI FOKOZAT MEGHATÁROZÁSA

Az államháztartás szervezete adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

Az államháztartás szervezete alapbiztonsági fokozatba tartozik, általános informatikai feldolgozást végez.

V. KAPCSOLÓDÓ SZABÁLYOZÁSOK

A jelen szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- az információs önrendelkezési jogról és az információ szabadságról szóló 2011. évi CXII. törvény
- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII törvény
- 62/1997. (XII.21.) NM rendelet az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről
- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési kézikönyv,
- Belső kontroll rendszer.
- Adatvédelmi és adatkezelési szabályzat

VI. 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.

VI.1. Környezeti infrastruktúra által okozott 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.

VI.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 jelszó gyakori *(napi, heti)* megváltoztatásának az elmulasztása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal 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.

VI.3. Tűzvédelem

A gépterem (szerverszoba) illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A tűzvédelem feladatait, sajátos előírásokat a gépteremre *(informatikai szobára)* vonatkozóan Az Intézet Tűzvédelmi szabályzata tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a gépterem és az adatállomány-tároló helyiség között.

Az államháztartás szervezete azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A gépteremben csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. leporellót).

A gépteremben dohányozni tilos.

A géptermekben, valamint a munkaállomásoknál ételt, italt fogyasztani tilos.

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

Ezen adatállományok kijelölése az adatvédelmi felelős *(rendszergazda)* feladata.

VII. A SZÁMÍTÁSTECHNIKAI ADATOK KÖZVETLEN VÉDELME

Az Intézet tulajdonában lévő rendszer és felhasználói programok védelme az Intézet törvényben előírt kötelessége.

Minden vásárolt vagy saját fejlesztésű program eredeti példányát és annak teljes kezelési dokumentációját a telepítés után tűzbiztos helyen, fémszekrényben kell tárolni. Ezen a helyen az adathordozót és a dokumentációt minimálisan 1 évig, de legalább addig meg kell őrizni, amíg a program használatban van.

A program használatból való kivonásáról az Informatika, mint szervezeti egység és a vezetőség közösen hoznak döntést. A használatból kivont programot dokumentációjával együtt a Központi Irattárba kell leadni és a főinformatikusnak gondoskodni kell a leltárból való kivezetéséről.

VIII. A PROGRAMOK BESZERZÉSÉNEK, TELEPÍTÉSÉNEK ÉS FRISSÍTÉSÉNEK SZABÁLYOZÁSA

Az új rendszer vagy felhasználói program kiválasztásáról a főigazgató által kijelölt testület dönt. Amennyiben a főigazgató nem jelölt ki testületet, úgy az intézeti adatvédelmi felelős, a fő informatikus és egy, a felhasználói programot közvetlenül használó vezető dönt a program elfogadásáról.

A megvásárolt programok telepítését és a meglévők frissítését csak a főinformatikus vagy az általa kinevezett személy (rendszergazda) végezheti el. Az új program telepítése során a forgalmazó köteles a telepítésre vonatkozó összes dokumentumot és információt maradéktalanul átadni a rendszergazdának olyan formában, hogy abból nélküle is maradéktalanul visszaállítható legyen a program az esetleges sérülés esetén.

Hálózati rendszerprogram telepítése előtt a főinformatikus vagy megbízottja köteles a szerver leállásáról legalább 1 nappal előbb értesíteni azokat az osztályokat, amelyeket az adatfeldolgozási kiesés közvetlenül érint, valamint a hálózaton a telepítés megkezdése előtt üzenetben felszólítani a kilépésre a hálózat alatt dolgozókat. Az installálás befejezéséről, a szerver újraindításáról telefonon értesíteni kell az érintett osztályokat, illetve meg kell győződni a helyes működésről.

IX. AZ INTÉZET HÁLÓZATI ÉS EGYEDI GÉPEINEK VÍRUSVÉDELMÉRE SZOLGÁLÓ INTÉZKEDÉSEK

Az intézeti gépeken csak az Intézet tulajdonát képező programok és adatbázisok futtathatók és kezelhetők. A gépek közötti adatcserét a hálózaton kell megoldani, illetve egyedi gép esetében ez a művelet csak az Intézet tulajdonát képező ellenőrzött adathordozón hajtható végre.

Az Intézet gépein saját adathordozót, illetve az intézeti adathordozót az Intézeten kívül használni tilos. Amennyiben mégis feltétlenül szükséges, úgy azt csak az informatikai vezető vagy a rendszergazda előzetes vírusellenőrzésével - vírusmentes állapotban - lehetséges.

Az Intézet informatikai hálózatára és egyedi gépeire bármilyen program, illetve adat telepítése csak vírusvizsgálat után lehetséges.

A főinformatikus vagy annak megbízottja köteles havi rendszerességgel a hálózaton és az egyedi gépeken külön-külön vírusellenőrzést végezni vagy végeztetni.

A vírusos állapot detektálásakor a vírusos programból el kell távolítani a vírust és a kereső újrafuttatásával detektálni kell a vírus mentés állapotot. Amennyiben a vírus nem távolítható el a programból, úgy a programot le kell törölni és az eredeti telepítőről újra kell telepíteni. Ha a vírus a program futását úgy módosította, hogy az adatok is megsérültek, úgy az adatokat a napi mentésekből vissza kell állítani. A teljes visszatelepítés után újra le kell futtatni, a vírusellenőrző újrafuttatásával pedig detektálni kell a vírusmentes állapotot.

A főinformatikus vagy a rendszergazda köteles a víruskereső és mentesítő program naprakész állapotáról gondoskodni.

X. A SZAMÍTÁSTECHNIKAI ADATOK LEMENTÉSÉNEK SZABÁLYOZÁSA

Az informatikai hálózat adatainak rendszeres mentéséért a főinformatikus a felelős. Az adatok mentése előre meghatározott időpontokban, az éjszaka folyamán történik.
A központi szerverek adatainak automatikus mentését napi rendszerességgel kell elvégezni.
A hálózaton kívül üzemelő számítógépek mentéséről az egység adatvédelmi felelőse köteles gondoskodni.

Az egyedi gépekről a mentést a munkanap befejezésekor kell elvégezni annak a dolgozónak, aki utoljára használja a számítógépet, minden nap más adathordozóra, heti ciklusokban ismételve azt.
A hálózati, illetve az egyedi mentések meghiúsulása esetén ki kell cserélni az adathordozót, és meg kell ismételni a mentést a hiba észlelésekor.
A hálózati mentett adatokat tartalmazó adathordozókat az informatika helyiségében tűzbiztos fémszekrényben kell tárolni. Ennek felelőse a fő informatikus.
Az egyedi számítógépek mentett adatainak adathordozóit, a gépet vagy gépeket üzemeltető szervezeti egység helyiségében, tűzbiztos lemezszekrényben kell tárolni. A tárolás biztosítása az egység adatvédelmi felelős feladata.

XI. INTÉZETI HÁLÓZATI SZOFTER LEÁLLÁSA ESETÉN ALKALMAZANDÓ TEENDŐK

Az intézeti hálózat folyamatos üzemű. A működésének fenntartása is ehhez kell, hogy igazodjon.

A rendszer leállásakor a leállást elsőként észlelő dolgozó értesíti az informatikusokat, akik elvégzik a szerver újraindítását. Ha a szerver meghibásodása olyan jellegű, hogy hosszabb kiesés várható, úgy az Intézetben aktuálisan ügyeletes orvos intézkedik az adatok hagyományos módszerrel történő vezetéséről.

A szerver újraindítása után, amennyiben adatvesztés történt, azonnal meg kell kezdeni az adatok visszatöltését a napi mentések felhasználásával. A visszatöltés után értesíteni kell az érintett osztályokat, hogy adataik milyen határidővel lettek visszatöltve. A felhasználók kötelesek egyeztetni adataikat a gépi adatokkal és a hiányzókat újra felvinni a számítógépes nyilvántartásba. A mentett adatok szerverbe való visszatöltéséért az informatikai vezető a felelős. Az adatok újra beviteléért az egység adatvédelmi felelős felel.

A hálózaton kívüli egyedi gépek adatvesztésének helyreállítását az informatika dolgozói végzik el, a szervezeti egységnél található napi mentések felhasználásával. Az adatok helyreállításáért és naprakészségéért az adatvédelmi felelős felel.

Áramszünet esetén, amennyiben arról a Műszaki Osztály előre értesül, kötelessége arról az informatikusokat haladéktalanul értesíteni, akiknek kötelességük az információt az érdekelteknek továbbítani. A továbbiakban úgy kell eljárni, mint a szerver leállásakor.

XII. A HÁLÓZATBA VALÓ ILLEGÁLIS BEHATOLÁS ESETÉN ALKALMAZANDÓ TEENDŐK

A hálózatba való illegális **behatolás fajtái**:

- a felhasználó által felismerhető illegális belépés. A hálózatba való illegális behatolásról akkor beszélhetünk, ha a rendszerbe való belépés után adataink megváltoztak, elvesztek, vagy a rendszerből egész adatbázisok, vagy annak részei eltűntek. Ilyenkor felmerül a gyanú, hogy illegálisan és a szándékos károkozás céljából léptek be a rendszerbe.

- a rendszergazda a hálózati szoftver adminisztrációs jelentéseiből megállapíthatja az illegális belépés tényét.

A felhasználó az illegális belépés gyanújáról köteles értesíteni a rendszergazdát és a helyszínen megvárni őt.

A rendszergazda a hálózati szoftver adminisztrációs jelentéseiből megállapítja, hogy hol, mikor, milyen USER néven léptek be illegálisan, és intézkedik az adatok helyreállításáról, valamint új jelszókiadását kezdeményezi a fő informatikusnál és a szervezeti egység vezetőnél, akik azt kötelesek haladéktalanul végrehajtani.

Amennyiben nem sikerül megállapítani, hogy a belépés hogyan történt, úgy a rendszergazda köteles a hálózat hosszabb idejű megfigyelésére, amíg az illegális belépőt pontosan be nem határolja. Az illegális belépés részletes felderítése után a rendszergazda köteles úgy megváltoztatni a rendszerkörnyezetet, hogy a további ilyen módon való belépést lehetetlenné tegye. A rendszerkörnyezet megváltozásáról értesíteni kell az érintett szervezeti egységek egység adatvédelmi felelőseit és a szervezeti egységek vezetőit, akik kötelesek a szervezeti egységükön belül a belépési jelszavaik megváltoztatására.

XIII. HÁLÓZATI BELÉPÉSI ÉS MUNKAVÉGZÉSI JOGOSULTSÁGOK SZAKMA SZERINTI CSOPORTOSÍTÁSA

Főigazgató

Belépési jogosultság olvasásra: minden rendszerbe.

Ápolási igazgató

Belépési jogosultság olvasásra: az egészségügyi rendszerbe.

Közgazdasági csoportvezető

Belépési jogosultság olvasásra és írásra: a gazdasági rendszerbe, olvasásra az egészségügyi rendszerbe.

Egyéb gazdasági ügyintézők, előadók

Belépési jogosultság olvasásra és írásra: a gazdasági rendszerbe.

Központi irányításvezető

Belépési jogosultság olvasásra és írásra: a gazdasági rendszerbe, olvasásra az egészségügyi rendszerbe.

Titkárság

Belépési jogosultság olvasásra és írásra: a gazdasági rendszerbe, olvasásra az egészségügyi rendszerbe, pathológia rendszer, iktató rendszer, ügyeleti rendszer.

Jogi referens

Belépési jogosultság olvasásra: a gazdasági rendszerbe, az egészségügyi rendszerbe.

Informatikusok

Belépési jogosultság írásra és olvasásra: a hálózat üzemben tartásához szükséges rendszer programok, valamint az összes felhasználói alrendszer.
Jelszó kiadási jog: van
Új felhazsnáló felvételi jog: van

Munka és bérügyi előadók

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer főkönyv, pénzügy rendszer moduljai. A munkaügy nyilvántartási rendszer moduljai.

Főgyógyszerész

Belépési jogosultság írásra és olvasásra: az egészségügyi rendszer gyógyszer alrendszer moduljai.

Gyógyszertári szakasszisztensek

Belépési jogosultság írásra és olvasásra: az egészségügyi rendszer gyógyszer alrendszer moduljai.

Osztályvezető főorvosok

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe, képalkotó programok.

Kezelőorvosok

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe, képalkotó programok.

Orvosok

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe, képalkotó programok.

Főnővérek

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe

Betegellátók (ápolási személyzet)

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe

Osztályos adminisztrátorok

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe, képalkotó programok, pathológiai nyilvántartás.

Labor főorvosok

Belépési jogosultság: pénzügyi gazdasági alrendszer osztályközi megrendelés, labor alrendszer írásra és olvasásra.

Labor asszisztens(ek)

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer osztályközi megrendelés és munkalap moduljai, labor alrendszer.

Röntgen főorvos

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe, képalkotó programok.

Röntgen asszisztens(ek)

Belépési jogosultság írásra és olvasásra: egészségügyi rendszerbe, képalkotó programok.

XIV. JELSZAVAK KIADÁSÁNAK RENDJE

Hálózati jelszónak nevezzük a hálózati-rendszer program illegális belépés megakadályozására, a program védelmére szolgáló jelszót. A hálózati jelszavakat két csoportra bontjuk, úgymint rendszergazdai és általános felhasználói jelszó.

A rendszergazdai jelszó birtokában a hálózat teljes adminisztrációja, paraméterezése, működése változtatható. A rendszergazda adja meg az új felhasználók jogosultságait.

A rendszergazdai jelszót ennek megfelelően titkosan kell kezelni. A jelszó csak a rendszergazda birtokában lehet, azt másnak ki nem adhatja.

A rendszergazda köteles a jelszó megváltoztatására azonnal, ha illegális behatolást észlelt a rendszerbe, és minden olyan esetben, amikor szükségesnek tartja. A régi jelszót tartalmazó borítékot a megőrzésért felelős köteles felbontás nélkül a rendszergazda jelenlétében megsemmisíteni.

Az általános felhasználói jelszavak nyilvántartásáról és karbantartásáról a rendszergazda gondoskodik.

A hálózatba minden osztály minden dolgozója saját osztályának nevével lép be, ami a munkakörétől függően az alábbi alrendszerekbe való belépéseket engedélyezi:

- INFOREND rendszer (fekvő- és járóbeteg terület),
- PHARMAGIC rendszer (gyógyszertár),
- ANDROMÉDA rendszer (laboratóriumi szakterület),
- PACS rendszer (képalkotó diagnosztikai szakterület),
- PATHOLOGIST rendszer (pathológia szakterület),
- ÜGYELETI NYILVÁNTARTÁS

- ECOSTAT rendszer (gazdasági terület),
- FIN rendszer (járó finanszírozás),
- KIRA rendszer (munkaügyi terület),
- KONTOLLER rendszer (iktatás)

Minden új dolgozó belépéséről köteles a szervezeti egység írásban értesíteni a rendszergazdát, aki a munkahelyének és beosztásának megfelelően felveszi őt új felhasználóként a rendszerbe, és felruházza a hozzáférési jogaival. A felhasználó az első belépés után definiálhatja saját belépési jelszavát, amit a rendszergazda sem tudhat.
A felhasználói jelszót annak tulajdonosa másnak nem adhatja ki.
A felhasználói jelszó tulajdonosa köteles jelszavát megváltoztatni abban az esetben, ha tudja, vagy gyanítja, hogy jelszavával visszaéltek.
A dolgozó kilépésekor felhasználói nevét és jelszavát a munkaügyi osztály jelentése alapján törölni kell a rendszerből.

A felhasználói programokon belüli jelszavak kiadása az informatikusok feladata.
Az új belépő a rendszergazda után köteles a szervezeti egység vezetőjénél jelentkezni, hogy a szervezeti egység által használt felhasználói programbeli jogosultságait megadja. A jogosultságok megszerzése után a dolgozó definiálja jelszavát, amit a szervezeti egység vezetője sem tudhat.
A jelszót annak tulajdonosa másnak nem adhatja ki.
A jelszó tulajdonosa köteles a jelszava megváltoztatását kezdeményezni a szervezeti egység vezetőjénél abban az esetben, ha tudja, vagy gyanítja, hogy jelszavával visszaéltek, de legalább negyedévente.

XV. EGÉSZSÉGÜGYI ÉS SZEMÉLYAZONOSÍTÓ ADATOK NYILVÁNTARTÁSA

Az érintettről felvett, a gyógykezelés érdekében szükséges egészségügyi és személyazonosító adatot, valamint azok továbbítását nyilván kell tartani.

Az **adattovábbítás ténye** az iktatás során rögzítésre kerül az alábbi tartalmi elemekkel:

- adattovábbítás címzettje,
- adattovábbítás időpontja,
- továbbított adatok köre (betegdokumentáció. Rtg. film, zárójelentés, stb.),
- adattovábbítás célja (alapdokumentum szerint),
- adattovábbító aláírása.

A kezelést végző az általa vagy az egyéb betegellátó által felvett egészségügyi adatokról, a saját tevékenységéről és intézkedéseiről feljegyzést készít, mely a betegdokumentáció részét képezi.

A **betegellátó nyilvántartja**:

- azokat az érintetteket, akikről bebizonyosodott vagy valószínűsíthető, hogy az 2. számú melléklet szerinti fertőző betegségben szenvednek. Ezzel összefüggésben nyilván kell tartani a megelőző gyógyszeres kezelésre, a szűrővizsgálatra, a járványügyi megfigyelésre, a járványügyi ellenőrzésre, a járványügyi zárlatra kötelezett személyeket,
- a védőoltásra kötelezett személyeket,
- azokat, akik kábítószer-élvezők, gyógyszert kóros mértékben fogyasztók, illetve egyéb, hasonló jellegű függőséget okozó anyagot használnak. Ezekre a személyekre vonatkozó egészségügyi és személyazonosító adatokat egymástól elkülönítetten kell tárolni.

A gyógyszerész nyilvántartást vezet az orvosi rendelvényre kábítószert igénybe vett érintettekről.

A különféle egészségügyi dokumentációk nyilvántartásával, megőrzésével, archiválásával, selejtezhetőségével kapcsolatosan az Intézet Iratkezelési Szabályzatában részletezett szabályok az irányadóak.

XVI. EGÉSZSÉGÜGYI ÉS SZEMÉLYAZONOSÍTÓ ADATOK TÁROLÁSÁNAK FELTÉTELEI

Az egészségügyi dokumentációknak kezelési gyakoriságuk szerint három szintjét különböztetjük meg. A különböző szintek és a hozzájuk kapcsolódó tárolási feltételek a következők:

„A" szintnek nevezzük a mindennapi kezelésre szoruló dokumentációkat. Ezek azok a dokumentációk, melyek a jelenleg is bent fekvő illetve vizsgálaton lévő érintettek iratait tartalmazzák. Ezeket a dokumentációkat az illetékes osztály/egység irodáján tárolják olyan helyen, hogy biztosítva legyen a kezelőorvos bármikori hozzáférhetősége, de védve legyen az érintett kezelésében részt nem vevők (pl. hozzátartozók, látogatók, fizikai dolgozók stb.) hozzáférhetősége ellen.

„B" szintnek nevezzük azokat a dokumentációkat, melyek öt irattári éven belüliek. Ezeket a dokumentációkat az osztály/egység kézi irattárában kell elhelyezni. A kézi irattár kialakításánál biztosítani kell a dokumentációk védelmét és hozzáférésük rendszerét. A kézi irattárba helyezett dokumentációkat nyilvántartási sorszámuk szerint kell raktározni biztonsági zárral ellátott tároló szekrényekben vagy biztonsági zárral ellátott helyiségben. A kézi irattározási feladatokat az osztályos adminisztrátor láthatja el. A kézi irattározó elhelyezi a dokumentációkat a kézi irattárban, igény esetén - az arra jogosult kérőnek - a raktári kölcsönzési naplóba történő bejegyzés után kölcsönzi a kért dokumentációt, illetve a Központi Irattárba helyezendő dokumentációkat a megfelelő nyilvántartókönyvekkel és átadási

jegyzőkönyvvel átadja az irattárosnak. A központi irattárból történő dokumentáció kölcsönzésére és a központi postázóból a napi posta átvételére is csak a kézi irattáros jogosult.

„C" szintnek nevezzük azokat a dokumentációkat, melyek egy irattári éven túliak. Ezeket a dokumentációkat a Központi Irattárban kell elhelyezni. A Központi Irattár kialakítására mindenképpen olyan helyiséget kell használni, ahol télen-nyáron biztosítható a megfelelő páratartalom (55-65%) és a 17-18 C hőmérséklet, tűz- és víz biztos helyen van, közművezeték nem halad át a helyiségen. Az irattárat stabil vagy mobil, vasból vagy acélból készült állványokkal kell berendezni úgy, hogy a hozzáférhetőség és a munkavédelmi szempontok biztosítva legyenek. A dokumentációk nyilvántartására szolgáló regisztereket külön dobozban kell tárolni, évek szerint.

A **regiszterek** kötelező jelző adatai:

- dokumentumazonosító szám (sorszám),
- beteg neve,
- betegazonosító,
- egység neve,
- felvétel és/vagy távozás dátuma.

A dokumentációkat archiváló dobozokban kell tárolni, a dobozokat a tartalmuk (évkör, egység, nyilvántartási szám –tól –ig, megőrzési idő) nyilvántartására szolgáló címkével kell ellátni. A nem papíralapú iratokat, az időtállóságot biztosító paramétereknek megfelelően kell tárolni. Az elektronikus adathordozók irattározásánál legfontosabb szempont a biztonsági másolatok készítése, melyet az eredetiektől elkülönített, de azzal azonos biztonsági feltételekkel kell tárolni.

A központi irattárból iratot csak az irattáros kölcsönözhet ki a raktári kölcsönzési napló és az iratpótló lap megfelelő vezetésével, az iratkölcsönzésre jogosult kézi irattárosok számára. (Az irat betekintésére jogosult dolgozók a kézi irattároson keresztül kérhetnek ki a központi irattárból iratot.)

XVII. INTERNET HOZZÁFÉRÉSSEL KAPCSOLATOS RENDELKEZÉSEK

Az internet eléréseket biztosító számítógépekre a helyi hálózatra nem kapcsolódó munkaállomásokra vonatkozó szabályok érvényesek.

Az internetes gépen minden esetben működtetni kell a vírusvédelmet.
A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.
A tűzfal működése közben keletkező állományokat az üzemeltetőnek rendszeresen ellenőrizni kell.

A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztését az a főigazgató főorvos szabályozza.

XVIII. AZ ELEKTRONIKUS LEVELEZÉS SZABÁLYAI

Minden alkalmazottnak lehetősége van internetes postafiókot igényelni.

Az államháztartás szervezete nem monitorozza a hálózatából küldött, illetve ide érkező levelek tartalmát.

Az elektronikus levelezés **alapelvei**:

- A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartásformát.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelek tartalma nem sérthet meg szerzői és szomszédos jogokat.
- A levelek nem ronthatják az államháztartás szervezete hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.
- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése illetve továbbküldése.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről az államháztartás szervezete levelező rendszerét e-mail szeméttel (spam) terhelhetik meg.

A hálózaton történő (titkosítás nélküli) levelezés nem biztonságos, könnyen megfigyelhető (akárcsak egy levelezőlap tartalma), ezért érzékeny információkat titkosítás nélkül soha ne küldjünk e-mailben.

Ismeretlen feladótól érkezet, különös témájú, csatolt fájlt tartalmazó levelekkel legyünk nagyon óvatosak, a jelek vírusfertőzésre utalhatnak, töröljük a levelet.

XIX. ELLENŐRZÉS

Az államháztartás szervezete éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.
Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.

A folyamatba épített előzetes, utólagos és vezetői ellenőrzés során a jelen szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

XX. EGYÉB RENDELKEZÉSEK

Telephelyeken készült adatszolgáltatásról (betegellátás havi jelentése) a telephely informatikusa az Intézet székhelyére a kísérőjegyzékről elektronikus úton másolatot továbbít.

XXI. ZÁRÓ RENDELKEZÉSEK

A jelen szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat, melyet a jelen szabályzat hatályba lépést követő 15 napon belül kell elvégezni.

A jelen szabályzatot szükség szerint, de legalább 3 évenként felül kell vizsgálni. A felülvizsgálatért felelős: főinformatikus.

A szabályzat hatályba lépésével egyidejűleg hatályát veszti a 2013. január 01. napjától hatályos Informatika biztonsági szabályzat.

Kapcsolódó adatlapok:

- ISZ-008-A/01: Elosztási lista
- ISZ-008-A/02: Megismerési nyilatkozat

A folyamatba épített előzetes, utólagos és vezetői ellenőrzés során a jelen szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

XX. EGYÉB RENDELKEZÉSEK

Telephelyeken készült adatszolgáltatásról (betegellátás havi jelentése) a telephely informatikusa az Intézet székhelyére a kísérőjegyzékről elektronikus úton másolatot továbbít.

XXI. ZÁRÓ RENDELKEZÉSEK

A jelen szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat, melyet a jelen szabályzat hatályba lépést követő 15 napon belül kell elvégezni.

A jelen szabályzatot szükség szerint, de legalább 3 évenként felül kell vizsgálni. A felülvizsgálatért felelős: főinformatikus

Kapcsolódó adatlapok:

- ISZ-008-A/01: Elosztási lista
- ISZ-008-A/02: Megismerési nyilatkozat

KOCH RÓBERT KÓRHÁZ ÉS RENDELŐINTÉZET A Debreceni Egyetem részjogú akkreditált szakorvos képző helye	ISZ-008-A/01
INFORMATIKA BIZTONSÁGI SZABÁLYZAT	Kiadás száma: 01
ADATLAP ELOSZTÁSI LISTA Hatályba lépés napja: 2017. február 01.	Oldalszám: 01

Példány ssz.	Elosztás helye / beosztás	Átvevő neve, munkaköre	Dátum	Aláírás
1.	Központi irányítás (eredeti példány)			
2.	Közgazdasági Csoport	MATESZ KINGA KÖZGAZD. CSOP. VEZ.	2017. 01.30.	
3.	Ápolási Igazgató	SZEPESI ÉVA	2017. 01.31	
4.	Gazdasági-műszaki Csoport	GYARMATI GÁBOR	2017 01.26	
5.	I. Tüdőosztály	TAKÁCS CSABÁNÉ	2017. 01.26	
6.	II. Tüdőosztály	DICSŐ MÁRIA	2017 01.26	
7.	III. Tüdőosztály	HAJDÚ ISTVÁNNÉ	2017. 01.26	
8.	Krónikus Belgyógyászat és Légzés Rehabilitáció	KORBÉLY KATALIN	2017 01.26	
9.	Tüdőgondozó	BÜRNÉ TÁBOR NOÉMI	2017 01.26	
10.	Röntgen, Ultrahang	TAKÁCS JÓZSEFNÉ	2017. 01.26	
11.	Labor	KISS ANDRÁSNÉ	2017 01.26	
12.	Légzőszervi Rehabilitációs Központ	ALMÁSI BARNABÁSNÉ	2016. 01.26.	
13.	Gyógyszertár	LIPTÁK KATALIN	2017 01.26	
14.	Élelmezés	HEISZMANN ÁGNES	2017. 01.26	
15.	Rendelőintézet Edelény, Deák Ferenc út	DUCSAI TINEA	2017. 01.31.	
16.	Pszichiátriai Szakkórház, Izsófalva	SZEPESI ÉVA	2017. 01.31.	