A NYÍREGYHÁZI EGYETEM INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Elfogadva:
2008. szeptember 23.
Utolsó módosítás:
2023. június 20., hatályba lép: 2023. június 22-én

A Nyíregyházi Egyetem Informatikai Biztonsági Szabályzata

A Nyíregyházi Egyetem Informatikai Biztonsági Szabályzata (a továbbiakban: IBSZ)az információs önrendelkezési jogról és az információszabadságról szóló többször módosított 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény alapján készült.

1. § A Szabályzat célja

(1) Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

(2) Az IBSZ célja továbbá:

a) a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,

b) az üzemeltetett informatikai rendszerek rendeltetésszerű használata,

c) az üzembiztonságot szolgáló karbantartás és fenntartás,

d) az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,

e) az adatállományok tartalmi és formai épségének megőrzése,

f) az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,

g) a munkaállomásokon lekérdezhető adatok körének meghatározása,

h) az adatállományok biztonságos mentése,

i) az informatikai rendszerek zavartalan üzemeltetése,

j) a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,

k) az adatvédelem és adatbiztonság feltételeinek megteremtése.

(3) A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

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

2. § A Szabályzat hatálya

(1) Az IBSZ személyi hatálya kiterjed a Nyíregyházi Egyetem (a továbbiakban: Egyetem) valamennyi alkalmazottjára és hallgatójára.

(2) Az IBSZ tárgyi hatálya

a) kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,

b) kiterjed az Egyetem tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,

c) kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési stb.),

d) kiterjed a rendszer- és felhasználói programokra,

e) kiterjed az adatok felhasználására vonatkozó utasításokra,

f) kiterjed az adathordozók tárolására, felhasználására.

3. § Az adatkezelés során használt fontosabb fogalmak

(1) *Érintett:* bármely információ alapján azonosított vagy azonosítható természetes személy.

(1a) Azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

(2) *Személyes adat:* az érintettre vonatkozó bármely információ.

(3) *Különleges adat:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

a) *Genetikai adat:* egy természetes személy örökölt vagy szerzett genetikai jellemzőire

vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.

b) *Biometrikus adat:* egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat.

c) Egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

(4) *Bűnügyi személyes adat:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, *illetve a bűncselekmények* felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

(5) *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.

(6) *Közérdekből nyilvános adat:* a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

(7) *Hozzájárulás:* az érintett akaratának önkéntes,határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez.

(8) *Adatkezelő:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

a) Közös adatkezelő: az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval.

(9) A*datkezelés:* 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.

a) B*űnüldözési célú adatkezelés:* a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – (a továbbiakban együtt: bűnüldözési cél) végzett adatkezelése

b) N*emzetbiztonsági célú adatkezelés:* a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése.

c) *Honvédelmi célú adatkezelés:* a honvédelmi adatkezelésekről szóló törvény, és a Magyar Köztársaság területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyar Köztársaság területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról, valamint jogállásukhoz kapcsolódó egyes rendelkezésekről szóló törvény hatálya alá tartozó adatkezelés.

(10) *Adattovábbítás:* az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

a) Közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása.

b) Nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.

(11) *Nyilvánosságra hozatal:* az adat bárki számára történő hozzáférhetővé tétele.

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

(13) *Adatkezelés korlátozása:* a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján.

(14) *Adatmegsemmisítés:* az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

(15) *Adatfeldolgozás:* az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

(16) *Adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel

(17) *Adatfelelős:* az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

(18) *Adatközlő:* az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi.

(19) *Adatállomány:* az egy nyilvántartásban kezelt adatok összessége.

(20) *Harmadik személy:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel. az adatfeldolgozóval, vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek.

(21) *EGT-állam:* az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez.

(22) *Harmadik ország:* minden olyan állam, amely nem EGT-állam.

(23) *Adatvédelmi incidens:* az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

(24) *Profilalkotás:* személyes adat bármely olyan – automatizált módon történő – kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul.

(25) *Címzett:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz.

(26) *Álnevesítés:* személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tárolt – további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni.

4. § Az IBSZ biztonsági fokozata

(1) Intézményünk alapbiztonsági fokozatba tartozik. Ez a személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

(2) Intézményünk általános informatikai feldolgozást végez.

5. § Védelmet igénylő, az informatikai rendszerre ható elemek

(1) Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

(2) 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.

6. § A védelem tárgya

(1) 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, illetve a törlésre szánt adatok felhasználásáig,
e) az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
f) a személyhez fűződő és vagyoni jogokra.

7. § A védelem eszközei

(1) 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.

8. § A védelem felelőse

(1) A védelem felelőse a mindenkori Informatikai Szolgáltató Iroda Iroda (a továbbiakban: ISzI) vezetője, az egységvezetők és a rendszergazdák.

(2) A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény egységvezetőinek kell gondoskodnia.

(3) Egységvezetőnek minősül ezen szabályzat keretein belül a szervezeti felosztásban az intézetigazgató, a központvezető, az irodavezető, a könyvtárigazgató, a gyakorlóiskola igazgatója és a tanárképzési főigazgató.

9. . § Az adatvédelemért felelősök feladatai

(1) ISzI irodavezető feladatai:

a) az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
b) javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
c) a Szervezeti és Működési Szabályzat és egyéb szabályzat adatvédelmi szempontból való véleményezése,
d) felelős az intézmény informatikai rendszer hardver eszközeinek karbantartásáért,
e) ellátja az adatkezelés és adatfeldolgozás felügyeletét,
f) ellenőrzi a védelmi előírások betartását,
g) az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
h) az adatvédelmi feladatok ismertetése,
i) a felhasználók számítógépén ellenőrzi a szoftverek használatának jogszerűségét,
j) ellenőri tevékenységét adminisztrálja,
k) ellenőri tevékenységéről rendszeresen, de legalább évente beszámol az Informatikai Bizottság előtt.

(2) Egységvezetők feladatai:

a) meghatározza a védett adatok körét,
b) ellátja az adatkezelés és adatfeldolgozás felügyeletét,
c) ellenőrzi a védelmi előírások betartását,
d) az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
e) az adatvédelmi feladatok ismertetése,
f) ellenőri tevékenységét adminisztrálja.

(3) Rendszergazda feladatai:
a) a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
b) gondoskodik a rendszer kritikus részeinek újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról,
c) gondoskodik a folyamatos vírusvédelemről,
d) a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
e) felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
f) feladata a védelmi eszközök működésének folyamatos ellenőrzése,
g) nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
h) folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
i) ellenőrzi a rendszer önadminisztrációját.

(4) Felhasználó feladatai
a) az általa létrehozott adatok mentésének biztosítása,
b) hozzáférési azonosítóinak és a hozzájuk tartozó jelszavainak titkosságának megőrzése.

10. § Az ISzI irodavezető ellenőrzési feladatai

(1) Az ISzI irodavezető ellenőrzési feladatai:
a) évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
b) rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
c) előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

11. § Az ISzI irodavezető jogai

(1) Az ISzI irodavezető jogai:

a) az előírások ellen vétőkkel szemben szabálytalanságkezelési eljárás kezdeményezésére tehet javaslatot a rektor illetve a kancellár felé,
b) bármely érintett szervezeti egységnél jogosult informatikai biztonsági ellenőrzésre,
c) betekinthet valamennyi iratba, amely az informatikai feldolgozásokkal kapcsolatos,
d) javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
e) adatvédelmi szempontból az informatikai beruházásokat véleményezi.

12. § Az Informatikai Biztonsági Szabályzat alkalmazásának módja

(1) Az IBSZ megismerését az érintett dolgozók részére az ISzI biztosítja, melyről nyilvántartást vezet.

13. § Az Informatikai Biztonsági Szabályzat karbantartása

(1) Az IBSZ-t az intézményi szervezeti, valamint az informatikai technikai változások miatt – egyéb rendelkezés hiányában, azok bekövetkeztekor – aktualizálni kell.
(2) Az IBSZ folyamatos karbantartása az ISzI irodavezető feladata.

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

(1) Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:
a) közlésre szánt, bárki által megismerhető adatok,
b) bizalmas, személyes adatok,
c) minősített, titkos adatok.
(2) Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik, illetve a központi intézményi rendszerekhez kapcsolódóan az informatikai egység biztonsági felelőse minősíti. A minősítést a (3) §-ban pontban található definíciók alapján kell végezni.
(3) Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.
(4) A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

(5) Alapelv, hogy mindenki csak ahhoz az adathoz juthasson hozzá, amire a munkájához szüksége van.

(6) 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.

(7) A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.

(8) A naplófájlok áttekintéséért, értékeléséért az informatikai egység biztonsági felelőse és a rendszergazdák a felelősek.

(9) Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt), valamint törlése során információkhoz jut, adatkezelési nyilatkozatot kell aláíratni. Ennek aláírásáig a dolgozó kizárható az informatikai szolgáltatások igénybevételéből. (1. sz. melléklet)

(10) Az adatkezelési nyilatkozat naprakészen tartásáért az egységvezetők a felelősek.

(11) A titkot képező adatok védelmét a feldolgozás – adattovábbítás, 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).

14 A. § Hozzáférési jogosultságok

(1) Az intézményi informatikai rendszerekhez hozzáférési jogosultságot igényelni vagy jogosultság változást kérni az Informatikai Szolgáltató Irodánál, az erre a célra rendszeresített digitális igénykezelő rendszerben, annak elérhetetlensége esetén papír alapú igénylőlapon lehet.

(2) A hozzáférési jogosultsági igényt az igénylő személy szervezeti egységének vezetője a digitális igénykezelő rendszerben vagy a papír alapú igénylőlapon igazolja, majd a Kancellár elbírálás után az igény jogosságát a digitális igénykezelő rendszerben elektronikus jóváhagyással, a papír alapú igénylőlapon aláírásával igazolja.

(3) A digitális igénykezelő rendszerben vagy az igénylőlapon található információk alapján a hozzáférési jogosultságok kiosztását, módosítását, illetve megvonását az Informatikai Szolgáltató Iroda erre a feladatra feljogosított munkatársai végzik.

15. § Az informatikai eszközbázist veszélyeztető helyzetek

(1) Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

16. § Környezeti infrastruktúra okozta ártalmak

(1) Elemi csapás:

a) földrengés,
b) árvíz,
c) tűz,
d) villámcsapás, egyéb vis major.

(2) Környezeti kár:

a) légszennyezettség,
b) nagy teljesítményű elektromágneses térerő,
c) elektrosztatikus feltöltődés,
d) a levegő nedvességtartalmának felszökése vagy leesése,
e) piszkolódás (pl. por).

(3) Közüzemi szolgáltatásban bekövetkező zavarok:

a) feszültség-kimaradás,
b) feszültségingadozás,
c) elektromos zárlat,
d) csőtörés.

17. § Emberi tényezőre visszavezethető veszélyek

(1) Szándékos károkozás:

a) behatolás az informatikai rendszerek környezetébe,

b) illetéktelen hozzáférés (adat, eszköz),
c) adatok, eszközök eltulajdonítása,
d) rongálás (gép, adathordozó),
e) megtévesztő adatok bevitele és képzése,
f) zavarás (feldolgozások, munkafolyamatok, hálózati forgalom).

(2) Nem szándékos, illetve gondatlan károkozás:

a) figyelmetlenség (ellenőrzés hiánya),
b) szakmai hozzá nem értés,
c) a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
d) a megváltozott körülmények figyelmen kívül hagyása,
e) vírusfertőzött adathordozó behozatala,
f) biztonsági követelmények és gyári előírások be nem tartása,
g) adathordozók megrongálása (rossz tárolás, kezelés),
h) a karbantartási műveletek elmulasztása.

(3) A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen, vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

(4) Károkozás esetén belső vizsgálatot kell végezni az ISzI irodavezető, az informatikai biztonsági felelős és az érintett egységvezető közreműködésével.

(5) Szándékos károkozás esetén azonnal minden további hozzáférés megakadályozása szükséges. Ezt az ISzI irodavezető javaslata alapján a kancellár rendeli el.

(6) A Büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 386. §-a szerinti „Védelmet biztosító műszaki intézkedés kijátszása”, vagy a Btk. 422. §-a szerinti „Tiltott adatszerzés”, vagy a Btk. 423. §-a szerinti „Információs rendszer vagy adat megsértése”, vagy a Btk. 424. §-a szerinti „Információs rendszer védelmét biztosító technikai intézkedés kijátszása” bűncselekmény gyanúja felmerülésének alapján az intézménynek az illetékes hatóság felé feljelentést kell tennie.

(7) A szándékos károkozás tényéről és a tett intézkedésről írásban kell tájékoztatni a kancellárt.

(8) Nem szándékos károkozás esetén meg kell határozni a kárt okozó felelősségének mértékét, és annak függvényében kell lefolytatni a szükséges fegyelmi eljárást.

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

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

(2) A rendszerek megvalósítása során előforduló veszélyforrások
   a) hibás adatállomány működése,
   b) helytelen adatkezelés,
   c) programtesztelés elhagyása.

(3) A működés és fejlesztés során előforduló veszélyforrások
   a) emberi gondatlanság,
   b) szervezetlenség,
   c) képzetlenség,
   d) szándékosan elkövetett illetéktelen beavatkozás,
   e) illetéktelen hozzáférés,
   f) 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 kancellárnak azonnal jelenteni kell,
   e) az informatikai eszközöket csak az egyetem alkalmazottjai, ill. a hallgatói jogviszonnyal rendelkező hallgatók használhatják,
   f) az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

(2) *Külső adathordozó*k:
   a) könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,

b) az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
c) a használni kívánt külső adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
d) a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
e) adathordozót más, külső szervezetnek átadni csak a kancellár engedélyével szabad,
f) a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

(3) *Elektronikus adattovábbítá*s:
a) Az intézmény hálózatára csak felhasználói azonosító birtokában szabad csatlakozni,
b) a levelezésben és elektronikus adattovábbításban felhasználói azonosító használata kötelező,
c) a felhasználói azonosítókat, digitális aláírásokat központilag az ISzI kezeli, és tartja nyilván,
d) hivatalos dokumentumot interneten közzétenni, harmadik fél felé továbbítani csak nem szerkeszthető formátumban szabad.

(4) Tűzvédelem:
a) A gépterem, illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
b) A tűzvédelem feladatait, a sajátos előírásokat a gépteremre, szerverszobára vonatkozóan az intézmény Tűzvédelmi Szabályzata tartalmazza.
c) A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
d) Az intézmény géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.
e) Az intézmény géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi szakreferens tudtával, ill. engedélyével szabad végezni.
f) A nagy fontosságú, pl. törzsadat-állományokat, adatbázisokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az egységvezetők feladata.)

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 eszközöket, berendezéseket és adatokat
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 üzemeltetést, karbantartást és szervizelést az ISzI informatikusai végezik.
d) A munkák szervezésénél figyelembe kell venni:
   - a gyártó előírásait, ajánlatait,
   - a tapasztalatokat.
e) Bármely számítógép, vagy számítástechnikai eszköz szétbontását (kivéve a garanciális gépeket) csak az ISzI informatikusai végezhetik el.

(3) Az informatikai feldolgozás folyamatának védelme:

a) Az adatrögzítés védelme:
   - adatbevitel hibátlan műszaki állapotú berendezésen történjen,
   - csak tesztelt adathordozóra lehet adatállományt rögzíteni,
   - a külső adathordozókat csak az e célra kialakított és megfelelő tároló helyeken szabad tartani,
   - az adatrögzítés szoftveres védelme: lehetőség szerint olyan szoftvereket kell vásárolni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
   - hozzáférési lehetőség:
     - a felhasználói azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
     - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését

ugyanaz a személy nem végezheti.
    - a szerverek rendszergazda jelszavait az ISzI rendszergazdái kezelik.
- az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

b) *A külső adathordozók nyilvántartás*a:

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

c) *Külső adathordozók tárolás*a:

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

d) *Az adathordozók megőrzés*e:

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá intézményünk Bizonylati szabályzatában és az Iratkezelési szabályzat és irattári tervében foglaltak alapján az adatkezelő határozza meg.

e) *Selejtezés, sokszorosítás, másolá*s:

A selejtezést az Egyetem felesleges vagyontárgyai selejtezésének szabályzata, valamint az Iratkezelési szabályzat és irattári terv alapján kell lefolytatni.

Selejtezéskor biztonsági intézkedésekkel kell megakadályozni, hogy a hibás informatikai eszközök adathordozói ellenőrizetlenül kerüljenek ki a szervezeten kívülre. Szintén 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.

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.

f) *Leltározás*:

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

g) Mentések, file-ok védelme:

- Az adatfeldolgozás után biztosítani kell az adatok mentését.
- A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése és a mentés biztonságos tárolása 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 mentési tartalmak meghatározásáért az egységvezetők, technikai végrehajtásáért a rendszergazdák a felelősek.

21. § Szoftver védelem

(1) Rendszerszoftver védelem:

Az ISzI-n keresztül biztosítani kell, hogy a rendszerszoftverek naprakész állapotban legyenek és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

(2) *Felhasználói programok védelme*:

a) 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.

b) Programok megőrzése, nyilvántartása:

- A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni az IBSZ 2. számú melléklete szerint.
- A számvitelről szóló többször módosított 2000. évi C. törvény értelmében intézményünknek 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.

- 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 az ISZI, illetve az egységvezetők a felelősek.

22. § A központi számítógépek és a hálózat munkaállomásainak működésbiztonsága

(1) Központi gépek:

a) Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.
b) A központi gépek 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 Informatikai Szolgáltató Irodát azonnal értesíteni kell.
c) Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal kell ellenőrizni működésüket.
d) Az intézmény informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
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 intézmény hálózatára hálózati eszközt csak az ISzI vezetőjének engedélyével szabad csatlakoztatni. Az engedély nélkül csatlakoztatott eszköz hálózati hozzáférését az észlelést követően azonnal meg kell szüntetni, az eszközt csatlakoztató személy ellen ezen szabályzat 11.§ (1) a) pontja alapján az eljárást le kell folytatni.

23. § Ellenőrzés

(1) Az intézmény 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 megismétlődjön.

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

24. § Záradék

(1) Jelen szabályzatot a Nyíregyházi Főiskola Szenátusa az I/2-2/126/2008.(szeptember 23.) számú határozatával, 2008. szeptember 24-i hatállyal fogadta el.
(2) Jelen szabályzatot a Nyíregyházi Főiskola Szenátusa az RH/61-76/2014. (július 33.) számú határozatával, 2014. július 24-i hatállyal módosította.
(3) Jelen szabályzatot a Nyíregyházi Főiskola Szenátusa az IHK/111-70/2015. (március 31.) számú határozatával, 2015. április 2-i hatállyal módosította.
(4) Jelen szabályzatot a Nyíregyházi Egyetem Szenátusa az IHK/37-46/2016. (február 29.) számú határozatával, 2016. március 2-i hatállyal módosította.
(5) Jelen szabályzatot a Nyíregyházi Egyetem Szenátusa az IHK/44-113/2023. (június 20.) számú határozatával, 2023. június 22-i hatállyal módosította.

Nyíregyháza, 2023. június 20.

A Szenátus nevében:

Dr. Szabó György
rektor

1. sz. melléklet

Nyíregyházi Egyetem

ADATKEZELÉSI NYILATKOZAT

Alulírott _____ (név) nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek. Az Informatikai Biztonsági Szabályzatban foglaltakat megismertem, megértettem. A Szabályzatban foglaltaknak megfelelően járok el.

Nyíregyháza, _____

_____

Aláírás

Kezelésembe tartozó adatok köre:

_____

_____

_____

_____

_____

_____

_____

Nyíregyháza, _____

_____

egységvezető

2. sz. melléklet

Nyíregyházi Egyetem

SZOFTVER NYILVÁNTARTÁS

Szoftver neve:_____

Szoftver gyártója:_____

Leltárszám:_____

Szoftver verziószáma:_____

Szoftver leírása:_____

_____

_____

Szoftver azonosító sorszáma, szériaszáma:_____

Szükséges hardver környezet:_____

_____

Szükséges operációs rendszer, szoftverkörnyezet:_____

_____

Licensz feltételei (kik, hányan, hány számítógépen, mettől, meddig használhatják):_____

_____

Szoftver típusa (OEM, frissítés):_____

_____

Darabszám:_____

Egyéb:_____

_____

_____

_____

Adatfelvétel időpontja:_____

_____

adatfelvevő aláírása