Hatály: 2020. X. 1-től

Nemzeti Közszolgálati Egyetem
Informatikai Biztonsági Szabályzat

Szenátusi döntés
Elfogadta a Szenátus a 102/2020. (IX.23.) számú határozatával.

2020.

Tartalomjegyzék

A Nemzeti Közszolgálati Egyetem (a továbbiakban: Egyetem) Informatikai Biztonsági Szabályzata (a továbbiakban: Szabályzat) az alábbiak szerint kerül megállapításra:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK
A Szabályzat célja
1. §

(1) A Szabályzat alapvető célja, hogy az elektronikus információs rendszerek (a továbbiakban: rendszer, rendszerek) használata, alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát. Meghatározza a biztonságos üzemeltetés alapvető szabályait, az ellenőrizhető informatikai környezet kialakításához szükséges feltételeket, a használathoz és üzemeltetéshez kapcsolódó magas szintű szabályokat, az alapvető biztonsági normákat és követelményeket.

(2) A Szabályzat előmozdítja az informatikai és kommunikációs eszközök előírásoknak megfelelő és biztonságos használatát, ezzel támogatva, hogy az Egyetem által kezelt információvagyon sértetlensége, bizalmassága és rendelkezésre állása biztosított legyen.

(3) Az Egyetem Informatikai Igazgatósága (a továbbiakban: INI) az Egyetem összes telephelyére kiterjedő informatikai és kommunikációs hálózatot (a továbbiakban: Hálózat) üzemeltet. Az Egyetem székhelyén és telephelyein strukturált és menedzselt hálózat működik, amely aktív, passzív és végponti elemekből áll.

(4) A Hálózat célja az Egyetem egyes szervezeti egységei, illetve a felhasználók között az információáramlás biztosítása, valamint egyéb informatikai és kommunikációs szolgáltatások nyújtása a felhasználók számára.

(5) A Szabályzat a fenti cél teljesülése érdekében rögzíti a rendszerekre és a rendszerekkel kapcsolatos tevékenységekre vonatkozó adminisztratív, fizikai és logikai követelmények teljesítésével összefüggő feladatokat, folyamatokat és felelősségeket.

2. §

A jelen Szabályzat alkalmazásában

a) *dőlt betűs szövegrészek: a fontosabb vonatkozó jogszabályi rendelkezések a jelen Szabályzat 3.§-ában foglalt rövidítések alkalmazásával;*

b) álló betűs szövegrészek: a Szabályzat rendelkezései.

A Szabályzat hatálya
3. §

(1) Jelen Szabályzat személyi hatálya kiterjed az Egyetem Hálózatát és informatikai szolgáltatásait használó felhasználókra és rendszergazdákra, tárgyi hatálya kiterjed a Hálózat teljes infrastruktúrájára, azaz a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére, a folyamatokra, a székhelyre és valamennyi telephelyre és a létesítményekre is. Felhasználónak minősülnek az Egyetem polgárai, illetve mindazok, akik oktatási, kutatási, tudományos, adminisztrációs és egyéb feladataikhoz állandó vagy

eseti jelleggel vagy szerződés alapján az Egyetem Hálózatát, informatikai szolgáltatásait használják. A Hálózat és informatikai szolgáltatások vonatkozásában az oktatók, a rendszergazdák, a hallgatók, és az egyéb felhasználók különböző jogosultságokkal és kötelezettségekkel rendelkezhetnek.

(2) Az Egyetemen minősített adatokra, valamint az azokat kezelő, feldolgozó, tároló rendszerekre, rendszerelemekre, infokommunikációs eszközökre és adathordozókra vonatkozó előírásokat az NKE Biztonsági Szabályzata a minősített adatok védelmére című szabályzat tartalmazza.

(3) Az Egyetemen a személyes adatok védelmére, valamint a közérdekű adatok kezelésére vonatkozó előírásokat a Személyes és közérdekű adatok védelméről, biztonságáról szóló szabályzata tartalmazza.

(4) A Neptun adatbázis üzemeltetésére és kezelésére vonatkozó szabályokat a Neptun Egységes Tanulmányi Rendszer Szabályzat tartalmazza.

(5) A Szabályzatot az alábbiakban felsorolt jogszabályokkal összhangban kell alkalmazni:
- *a)* az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.),
- *b)* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.),
- *c)* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet,
- *d)* a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény,
- *e)* a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet,
- *f)* az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet,
- *g)* a minősített adat védelméről szóló 2009. évi CLV. törvény,
- *h)* az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR).

(6) Figyelembe veendő szabványok:
- *a)* MSZ EN ISO 9000:2015 Minőségirányítási rendszerek. Alapok és szótár,
- *b)* MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Alapok és követelmények,
- *c)* ISO/IEC 27000:2014 Information technology – Security techniques – Information security managements systems. Overview and vocabulary,
- *d)* MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények,
- *e)* MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek,

f) ITIL. (Information Technology Infrastructure Library) informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló kormányzati ajánlás, „de facto" szabvány.

Értelmező rendelkezések
4. §

GDPR 4. cikk „1. „személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;"
Info tv. 3.§ 5. pont „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."
Info tv. 3. § 6. pont „Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli."

1. Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
2. Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.
3. Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.
4. 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.
5. Adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzé teendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.
6. Adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.
7. 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 rögzítése.

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 határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza, valamint végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.
9. Aktív hálózati eszköz: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok (Acces Pointok), és egyéb eszközök (bridge-ek, tűzfalak, médiakonverterek, modemek, multiplex, rádiórelék, stb.), amelyek segítségével a Hálózat üzemvitele biztosítható.
10. Asztali munkaállomás: a felhasználó rendelkezésére bocsátott számítástechnikai eszköz, mely alapvetően a számítógépből, monitorból, billentyűzetből és egérből, illetve más csatlakoztatható számítástechnikai eszközökből (különösen: mikrofon, kamera, scanner, nyomtató stb.) állhat.
11. Belső Képzési Portál: az egyetemi oktató anyagok, a digitális oktatással kapcsolatos tájékoztatók, útmutatók, oktató videók elhelyezésre szolgáló felület.
12. Bizalmasság: az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról, valamint az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
13. Biztonság: a rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.
14. Biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
15. Biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.
16. (Bring Your Own Device – BYOD): saját infokommunikációs eszköz munkahelyi környezetben való használata.
17. Digitális Oktatási Portál (DOP): az Egyetem egységes, központi távoktatási felülete. https://digioktatas.uni-nke.hu/
18. Domain név: tartománynév (műszaki azonosító), amelyet elsősorban a könnyebb megjegyezhetősége miatt, az internetes kommunikációhoz nélkülözhetetlen cím tartományok (IP címek) helyett használnak. Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés, a számítógépek azonosítására szolgáló névtartomány (például: uni-nke.hu).
19. DNS (Domain Name System): az internet neveket és címeket egymáshoz rendelő adatbázis, amely általában külön kiszolgáló gépen fut.
20. Elektronikus információs rendszer (EIR): az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese (Ibtv. 1. § 14b. pont).
21. Felhasználó: az a természetes személy, aki az egyetemi informatikai infrastruktúrát használja.

22. Felhasználói azonosító: az egyetemi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.
23. Felhőszolgáltatás: olyan információs társadalommal összefüggő szolgáltatás, amely lehetővé teszi konfigurálható számítási erőforrások – különösen hálózatok, kiszolgálók, tárolók, alkalmazások, szolgáltatások – osztott készletének igény szerinti, hálózaton keresztül történő elérését. Ezen szolgáltatásokat nem az Egyetem hardvereszközein üzemeltetik, hanem az üzemeltetés részleteit a felhasználótól elrejtve a szolgáltató eszközein elosztva vannak. A szolgáltatásokat publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy ugyancsak az interneten érik el a felhasználók. Felhőszolgáltatás esetében az Egyetem nem szolgáltató és nem üzemeltető.
24. Hálózat: felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító passzív és aktív eszközökből álló infrastruktúra.
25. Hitelesség: az információ akkor hiteles, ha az elvárt, hozzáértő, megbízható forrásból származik.
26. INI Service Desk: az INI panasz, hiba- és eszközigényléssel foglalkozó része.
27. Informatikai erőforrások: a hardver, szoftver eszközök összessége.
28. Internet: a világháló.
29. Intranet: az intézményen belüli Hálózat és annak szolgáltatásai.
30. IP telefónia: olyan számítógép-hálózati alkalmazás, amely telefonszolgáltatást tesz lehetővé, ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.
31. Központi címtár: az Egyetem dolgozóinak felhasználói adatait tároló LDAP adatbázis.
32. Központi szolgáltatások: az Egyetem által nyújtott levelezés, címtár, fájl kiszolgálás, web szolgáltatás, névszolgáltatás, és más informatikai és kommunikációs szolgáltatások.
33. Kritikus adat: a GDPR szerinti személyes adat, különleges adat vagy valamely jogszabállyal, egyetemi szabályzattal védett adat.
34. LDAP (Light Weight Directory Access Protocol): nyílt szabványú címtár struktúra leírónyelv.
35. Ludovika Webinár: digitális oktatást támogató virtuális oktató/webinar előadó helyiségek (egyedi diszponálás útján biztosított olyan tantermek, ahol az előadások felvétele, esetenként on-line streamelésére van lehetőség) előadásainak tárhelye. https://ludovikawebinar.uni-nke.hu/
36. Mobil eszközök: notebook, netbook, tablet, palmtop, okostelefon.
37. Moodle: távoktatási rendszer, hallgatók, oktatók központi szervező felülete. https://moodle.uni-nke.hu/
38. Munkatárs: az Egyetemmel közalkalmazotti jogviszonyban vagy munkaviszonyban álló személy, az Egyetemre vezényelt és kirendelt személy, valamint az Egyetemmel munka-végzésre irányuló egyéb (különösen megbízási) jogviszonyban álló személy.
39. NEPTUN kód: a NEPTUN rendszerszolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló, legalább 6 karakter hosszúságú kód.
40. NIIFI program: a program a teljes magyarországi kutatási, felsőoktatási és közgyűjteményi közösség számára biztosít integrált országos számítógép-hálózati infrastruktúrát, valamint az erre épülő kommunikációs, információs és kooperációs szolgáltatásokat, élvonalbeli alkalmazási környezetet, és tartalom-generálási illetve tartalom-elérési hátteret.
41. O365 portál: az Office 365 felhőszolgáltatások elérésének központi oldala. A hallgatók és az oktatók egyaránt ezen a felületen lehetőséget kapnak az MS Office termékek on-line eléréséhez.
42. Okostelefon: internetezésre és/vagy dokumentumkezelésre is használható mobil telefon.

43. Hálózati passzív eszközök: a hálózati kábelezés, rendező-, és csatlakozó pontok összessége, valamint minden olyan egyéb eszköz, amely aktívan nem befolyásolja az adatok, üzenetek célba juttatási útvonalát.
44. PDCA: plan – tervezés, do – cselekvés, check – ellenőrzés, act – beavatkozás.
45. PDCA-ciklus: egy ismétlődő, négylépéses menedzsment módszer, amelyet a termékek és folyamatok kontrolljára és folyamatos fejlesztésére használnak.
46. Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók legyenek.
47. Rendszergazda: hálózati szolgáltatást nyújtó számítógép adminisztrátora.
48. Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
49. Szerver-feladatokat ellátó eszköz: olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.
50. Szerverhelyiség: fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol az informatikai erőforrások számára a folyamatos működés feltételei biztosítottak.
51. Szervezeti rendszergazda: az egyes egyetemi szervezetek felügyeletében lévő hálózati szolgáltatást nyújtó számítógép adminisztrátora.
52. Tűzfal: olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is.
53. Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges. Amennyiben az adattörlés előre megírt automatizmussal történik úgy nem szükséges adattörlési jegyzőkönyv felvétele.
54. Végfelhasználói eszköz: minden olyan informatikai eszköz, amely nem a központi rendszerek működtetésére használt eszköz.
55. VLAN: a Hálózat egy – a feladatoknak megfelelő, logikailag elkülönülő – meghatározott része. A VLAN-ok biztonsági feladatot is ellátnak, mivel elválasztják egymástól a részhálózatokat, ezzel biztosítva, hogy sérülés vagy támadás esetén csak az adott részterületre korlátozódjék az esetleges kár.
56. VPN szolgáltatás: speciális hálózati elérés (un. Virtuális magánhálózat), amely az Egyetem hálózatához történő bizalmas Hálózatához titkosított, és hitelesített kapcsolódást tesz lehetővé a világ bármely részéről (egy, az Egyetemtől függetlenül üzemeltetett, az Internetre csatlakoztatott hálózatból). Két típusa létezik: felhasználói VPN (munkatársak távoli kapcsolódására), illetve az un. „site-to-site” VPN (távoli telephelyek kapcsolódására).
57. WEB adminisztrátor: az Egyetem webszerverét működtető, vagy az Egyetem honlapjának felügyeletét ellátó személy. A web-es adat- és tartalomszolgáltatást az Egyetem szervezeteiből kijelölt felelősök végzik.
58. WiFi (Wireless Fidelity), WLAN: szabványos vezeték nélküli adatátviteli technika. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság).

Alapelvek
5. §

(1) A rendszerekkel, infokommunikációs eszközökkel és adathordozókkal kapcsolatos fejlesztői, üzemeltetői, biztonsági, továbbá felhasználói tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, üzemeltetési és védelmi előírásokat úgy kell meghatározni és dokumentálni, hogy azok garantálják az információbiztonság szükséges és elégséges szintjét.

(2) Az Ibtv. 5. §-a alapján az elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

(3) Kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni.

(4) A fenti tevékenységek szabályozását úgy kell kialakítani, hogy a tevékenységek megtervezéséért és végrehajtásáért való felelősséget minden esetben meg lehessen állapítani.

(5) Az Egyetem működésével összefüggésben keletkezett adatokkal az Egyetem rendelkezik jogszabályban vagy egyetemi szabályzatban meghatározott kivétellel.

A szabályozás rendszere
6. §

(1) Az Egyetem elkötelezett, hogy olyan informatikai biztonsági rendszert épít ki, ami folyamatszemléletű megközelítésen alapul. Az informatikai biztonsági rendszer alapját a PDCA ciklus és a kockázatalapú gondolkodásmód képezi, így lehetővé válik a követelmények megértése és következetes teljesítése, a folyamatok átgondolása, nyomon követése és folyamatos korrekciója, fejlesztése az eredményes működés érdekében.

(2) Jelen Szabályzat az informatikai biztonsági szabályozás alapdokumentuma, amely átfogóan és keretjelleggel szabályozza az információbiztonsági szempontból releváns kérdéseket, területeket a 3. § (5) bekezdésében felsorolt jogszabályi előírásoknak, követelményeknek megfelelően. A Szabályzatot a vezetői megbízása keretében az INI igazgatója (az elektronikus információs rendszer biztonságáért felelős személy előkészítése alapján) készíti el és gondozza.

(3) Az informatikai biztonsági és infokommunikációs szabályozás tárgykörébe tartozó részletes előírásokat a tematikus szabályzatok, a rendszerüzemeltetési szabályzatok/kézikönyvek tartalmazzák. A szabályzatok kiadmányozása:

a) rektori utasítás formájában kerül kiadásra:
  aa) a végfelhasználói eszközök szabályzata;
  ab) az informatikai kockázatkezelési szabályzat;
  ac) az informatikai kockázatkezelési terv;
  ad) az informatikai rendszerek üzemeltetésére vonatkozó szabályzat;

ae) videokonferencia használati szabályzat;

b) a fejlesztési ügyekért felelős rektorhelyettes által kiadott körlevél formájában kerül kiadásra a szerződéses felekkel szemben támasztott a szerződésekben érvényre juttatandó és a fejlesztések során alkalmazandó információbiztonsági szempontú követelmények kialakítása;

c) INI igazgatói hatáskörben kerülnek meghatározásra az INI állományára vonatkozóan:

ca) az informatikai fejlesztési és tesztelési szabályok;

cb) az informatikai hálózat és alkalmazások üzemeltetésére vonatkozó részletes szabályok;

cc) az informatikai szolgáltatás folytonossági terve;

cd) a gépterem használati szabályok;

ce) a jogosultsági és hozzáférési szabályok;

cf) incidenskezelési és biztonsági események kezelésére vonatkozó részletes szabályok;

cg) az INI belső dokumentumkezelési és folyamatmenedzsment szabályai;

ch) a katasztrófahelyzet esetén alkalmazandó helyreállítási terv;

ci) informatikai mentési szabályok;

cj) a vírusvédelmi szabályzat és adatmentesítési szabályok;

ck) az informatikai licence-gazdálkodásról szóló szabályok;

cl) új belépők és kilépők informatikai vonatkozású be- és kiléptetési szabályai;

cm) az informatikai folyamatleírások, amelyek tartalmazzák

- a készítő nevét, beosztását, munkakörét,
- a jóváhagyó nevét, beosztását,
- a készítés keltét,
- az alkalmazók körét,
- az érintett rendszer, szolgáltatás megnevezését,
- a munkafolyamat(ok), eljárásrend(ek) leírását.

(4) A 3. § (6) bekezdésében felsorolt szabványoknak való megfelelési törekvés és a folyamatos fejlesztés érdekében az INI – a (3) bekezdés c) pontján túlmenően – saját működését meghatározó, egyben az Egyetem részére nyújtott szolgáltatások minőségét garantáló további szabályokat – így különösen informatikai menedzsment kézikönyv, informatikai integrált irányítási szabályok és információbiztonsági irányítási rendszerre vonatkozó szabályok – állapíthat meg.

(5) A folyamatleírásokat az informatikai szakterület a saját dokumentumtárában tárolja és teszi elérhetővé az érintettek számára. A folyamatleírások naprakészségéről az INI irodavezetői gondoskodnak.

Információbiztonsági kockázatfelmérés és –kezelés
7. §

(1) Az Egyetem működése során használt rendszerek esetében a kockázatfelmérést szabványok és jogszabályok e paragrafusban hivatkozott dokumentumok alapján kidolgozott, Elektronikus információs rendszerek kockázatkezelési szabályzata határozza meg.

(2) A kockázatkezelési szabályzat egyértelműen tartalmazza:

a) kockázatok azonosítás szabályait,

b) vagyonelemek azonosításának szabályait,
c) fenyegetés katalógust,
d) védelmi intézkedés katalógust,
e) sebezhetőség katalógust,
f) hatások, következmények azonosítását,
g) kockázatok becslését, kockázatértékelést,
h) kockázatkezelést,
i) az információbiztonsági kockázatok monitorozását és felülvizsgálatát.

(3) A kockázatfelmérést követő kockázatkezelésre vonatkozó javaslatokat a kockázat kezelési tervet az INI igazgatójának bevonásával az elektronikus információs rendszerek biztonságáért felelős személy állítja össze.

(4) A rektor által jóváhagyott kockázatkezelési terv végrehajtásáról az érintett szakterületek gondoskodnak.

A védelmi intézkedések
8. §

(1) A rendszerhez rendelt védelmi intézkedések tervezése és teljesítése az elektronikus információs rendszerek 3. § (5) bekezdésében felsorolt jogszabályi előírásoknak, követelményeknek megfelelően és a kockázatkezelési szabályzat alapján történik.

(2) A működés során használt rendszerek esetében a még meg nem valósított vagy részlegesen megvalósított védelmi intézkedések teljesítésének tervezése a rendelkezésre álló erőforrások figyelembe vételével történik. A még meg nem valósított vagy részlegesen megvalósított védelmi intézkedések teljesítésének tervezésére vonatkozó adatokat az éves pénzügyi tervezés során szerepeltetni kell. A tervezésért az üzemeltetésért felelős szervezeti egység felelős.

(3) Az egyes rendszerek esetében a speciális, rendszer szintű védelmi intézkedésekre vonatkozó előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

II. FEJEZET
ELLENŐRZÉS ÉS ÉRTÉKELÉS
9. §

(1) Az egyes rendszerek esetében a folyamatba épített ellenőrzésekre vonatkozó előírásokat a rendszerüzemeltetési szabályzat/ kézikönyv tartalmazza.

(2) Az egyes rendszerekre vonatkozó védelmi intézkedések megfelelőségéről amennyiben szükséges független értékelők által végrehajtott ellenőrzésekkel (külső auditok) kell meggyőződni. Külső audit végrehajtására javaslatot tehet a rendszer fejlesztésében érintett informatikai szakterület vezetője (a fejlesztés alatt, illetve a fejlesztés lezárásakor), a rendszer üzemeltetésében érintett informatikai szakterület vezetője (üzembe adás előtt vagy üzemeltetés alatt), az INI igazgatója, az elektronikus információs rendszerek biztonságáért felelős személy. A külső audit végrehajtását a fejlesztési ügyekért felelős rektorhelyettes engedélyezi vagy rendeli el.

(3) A külső auditokról az INI nyilvántartást vezet, amely tartalmazza a külső audit:

a) tárgyát, beleértve az érintett rendszer, szolgáltatás megnevezését is,
b) időpontját,
c) végrehajtóját (szervezet megnevezése, munkatársak neve),
d) végrehajtásában közreműködő szervezeti egység megnevezését és a végrehajtásában közreműködő munkatársak nevét,
e) végrehajtására vonatkozó szerződés, megállapodás azonosító adatait,
f) megállapításait,
g) megállapításai alapján készített intézkedési terv adatait (azonosító szám, készítő, jóváhagyó, végrehajtási határidők),
h) a dokumentumok másolati példányát.

(4) A külső auditok során az auditor számára az audit sikeres végrehajtásához szükséges adatok, dokumentumok megismerését (betekintést) biztosítani kell. Az auditor számára dokumentumok átadása (papíralapon vagy elektronikusan) csak átadás-átvételi jegyzőkönyvvel történhet. Közérdekű vagy közérdekből nyilvános, továbbá nyílt adatok, dokumentumsablonok továbbítása e-mailen is történhet. Az auditor számára csak betekintés biztosítható az alábbi adatkörökbe és dokumentumtípusokba (a dokumentumok, adatok nem adhatók át):
a) a rendszer teljes logikai vagy fizikai rendszerterve,
b) a privilegizált jogosultságok kezelésére vonatkozó leírás,
c) paraméterezési adatok (amennyiben nem gyártó által közzétettek),
d) telepítési leírás (amennyiben nem gyártó által közzétett),
e) személyes adatokat tartalmazó adatállomány.

(5) Amennyiben a külső audit személyes adatokat érint, az auditor és az Egyetem között adatfeldolgozási szerződést kell kötni.

III. FEJEZET
AZ INFORMATIKAI BIZTONSÁG SZERVEZETE
Az INI igazgatója
10. §

Az INI igazgatója
a) felelős az Egyetem informatikai tevékenységének jogszerűségért, beleértve az informatikai biztonsági tevékenységet,
b) gondoskodik az informatikai biztonság személyi és tárgyi feltételeinek biztosításáról,
c) gondoskodik – szabályozás és ellenőrzés útján – az Ibtv.-ben és a kapcsolódó jogszabályokban előírt, információbiztonsággal összefüggő tevékenységek végrehajtásáról,
d) informatikai biztonsági kérdésekben dönt,
e) informatikai biztonsági fórumokon, közvetlenül vagy kijelölt munkatársa útján az Egyetem nevében részt vesz,
f) ellátja az Egyetem vonatkozásában az informatikai biztonsági szakmai irányítási és felügyeleti feladatokat, előkészíti a Szabályzatot, gondoskodik naprakészen tartásáról és oktatásáról,
g) gondoskodik – az érintett szakterületek bevonásával – az információbiztonsággal összefüggő felsővezetői döntések előkészítéséről,

h) közreműködik – az informatikai biztonsági szempontok meghatározásával – az informatikai biztonsággal összefüggő informatikai szakmai döntések előkészítésében,
i) kijelöli az INI adatvédelmi kapcsolattartóját,
j) kijelöli az INI állományából az biztonsági esemény kivizsgálásáért felelős munkacsoportot (a továbbiakban: Munkacsoport).

Informatikai Irodavezető(k)
11. §

Az Informatikai Irodavezető(k)
a) gondoskodik a rendszerek és a bennük kezelt, feldolgozott, tárolt adatok zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosításához szükséges intézkedések megtervezése, megvalósítása, ellenőrzése és szükséges korrekciója érdekében szükséges feladatok végrehajtásáról,
b) felelős – hatáskörük keretein belül – az irányítása alá tartozó szervezeti egységek által üzemeltetett vagy fejlesztett rendszerek jogszerű és szakszerű működéséért, működtetéséért, a rendszerekre vonatkozó informatikai szakmai és információbiztonsági előírások teljesítéséért, a hatályos belső szabályzatok és a bevált gyakorlatok érvényesítéséért,
c) kezdeményezi az irányítása alá tartozó szervezeti egységek tevékenységével érintett rendszerekkel összefüggő informatikai szakmai és információbiztonsági intézkedéseket, beszerzéseket, illetve közreműködnek azok végrehajtásában,
d) az informatikai biztonsággal összefüggő ellenőrzéseket tervez és hajt végre, illetve gondoskodik az ellenőrzések lefolytatásáról,
e) az informatikai biztonság megsértésének észlelése esetén azonnal jelenti azt az INI igazgatójának és javaslatot tesz az elektronikus információs rendszerek biztonságáért felelős személynek a megteendő intézkedésekre.

A rendszer működtetéséért felelős szervezeti egység vezetője, az adatgazda
12. §

A rendszer működtetéséért felelős szervezeti egység vezetője, az adatgazda
a) felelős a rendszer használatára vonatkozó szakmai szabályok meghatározásáért és írásbeli rögzítéséért, beleértve az üzletmenet-folytonosság biztosításával kapcsolatos – hatáskörébe tartozó – tervezési és szabályozási feladatokat is,
b) ellátja a rendszer használatához szükséges jogosultságok kezelésével kapcsolatos, számára meghatározott – irányítói – feladatokat,
c) meghatározza a rendszer által kezelt, feldolgozott, tárolt adatok körét, típusát, őrzési idejét,
d) javaslatot tesz a rendszer fejlesztésére, módosítására, kivonására.

Elektronikus információs rendszer biztonságáért felelős személy
13. §

(1) A rektor által kijelölt, az elektronikus információs rendszer biztonságáért felelős személy felel az Egyetemnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
c) előkészíti az Egyetem elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d) ha szükséges előkészíti az Egyetem elektronikus információs rendszereinek biztonsági osztályba sorolását és az Egyetem biztonsági szintbe történő besorolását,
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit.

(2) Az elektronikus információs rendszer biztonságáért felelős személy az elektronikus információs rendszereket érintő biztonsági eseményről haladéktalanul tájékoztatni köteles a rektort.

IV. FEJEZET
AZ INFORMATIKAI BIZTONSÁG VESZÉLYEZTETÉSE, MEGSÉRTÉSE
14. §

(1) A Szabályzat, a vonatkozó jogszabályok, belső szabályzatok be nem tartása, valamint az informatikai biztonság veszélyeztetése, megsértése esetén a felhasználóval szemben fegyelmi, illetve büntetőjogi felelősségre vonásnak lehet helye.

(2) Az előírások be nem tartásával okozott kárért való felelősségre vonatkozó rendelkezéseket az Egyetem szabályzatai tartalmazzák.

V. FEJEZET
SZERVEZETI BIZTONSÁGI KÖVETELMÉNYEK
Összeférhetetlen szerepkörök és feladatok szétválasztása
15. §

(1) Az informatikai és az informatikai biztonsági feladatokat ellátó szervezeti egységeket szervezeti szinten el kell különíteni.

(2) Az informatikai szerepkörök és feladatok szervezeti egységre és személyre (véglegesen vagy átmeneti időszakra történő) telepítését úgy kell végrehajtani, hogy a fejlesztési, üzemeltetési, ellenőrzési feladatok ellátásának egymástól való függetlensége biztosított legyen.

Helyettesítés
16. §

Az informatikai és az informatikai biztonsági szerepkörök és feladatok személyre telepítésekor a közvetlen vezető köteles gondoskodni a helyettesítésről.

Projektműködésre vonatkozó rendelkezések
17. §

Az Egyetem informatikáját érintő projektekben az INI igazgatója által kijelölt személy részvételét az irányítási és az operatív szinten is biztosítani kell.

VI. FEJEZET
SZEMÉLYI BIZTONSÁGI KÖVETELMÉNYEK
18. §

(1) A jogtalan hozzáférés, információvesztés és rongálás elkerülése érdekében alkalmazni kell a *„tisztaasztal, tisztaképernyő”* szabályt, azaz az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat, amennyiben annak feltételei adottak. Külön figyelmet kell fordítani és messzemenően be kell tartani az információk/adatok minősítésére vonatkozó előírásokat.

(2) A nyomtatókról azonnal el kell távolítani a kinyomtatott iratokat.

(3) Az aktuálisan nem használt számítógépet ki kell kapcsolni vagy jelszóvédetten kell zárolni.

Információbiztonsági képzés, továbbképzés
19. §

(1) Az Egyetemre új belépő munkatársat, a munkába állásának kezdetekor, de legkésőbb 3 hónapon belül a Szabályzat tartalmát megismertető, a biztonsági események jelentési kötelezettségére is figyelmeztető, továbbá az információbiztonsági tudatosság növelését is célzó képzésben kell részesíteni.

(2) Az információbiztonságra vonatkozó jogszabályi környezet megváltozásakor, továbbá ha az Egyetem informatikai biztonságát, illetve a jelen Szabályzat tartalmát érintő jelentős változás következik be, a jogszabályváltozás hatályba lépését, illetve a jelentős változást követő 60 napon belül a munkatársakat információbiztonsági továbbképzésben kell részesíteni.

(3) Az Egyetemmel polgári jogi jogviszonyban álló munkatársakat információbiztonsági tájékoztatásban kell részesíteni.

(4) Az informatikus munkakört, szerepkört, feladatkört ellátó munkatársak – előző bekezdésekben foglaltakon túli, munkakör, szerepkör vagy feladatkör alapú – képzéséről, továbbképzéséről az INI igazgatója gondoskodik a rendelkezésre álló erőforrások függvényében.

(5) Információbiztonsági képzés tananyagáért a továbbképzések megtartásáért az elektronikus rendszerek biztonságáért felelős személy a felelős.

VII. FEJEZET
INFORMATIKAI BIZTONSÁGI FELADATOK ÉS FELELŐSSÉGEK MEGHATÁROZÁSA
20. §

(1) A biztonságos informatikai szolgáltatások nyújtása érdekében az INI kötelezettségei:
- *a)* az oktatás, kutatás, tudományos munka informatikai támogatása, valamint az Egyetem Informatikai rendszereinek működtetése, továbbá a belső hálózati szolgáltatásokat, valamint az Egyetem internetes megjelenését, kapcsolattartását biztosító rendszerek folyamatos üzemeltetése;
- *b)* a Hálózat üzembiztosságának fenntartása, a hatályos szabályzatok, korlátozások betartásával elhelyezett adatok védelme;
- *c)* a Hálózat folyamatos karbantartása, fejlesztése, a lehetőségek mértékében a felmerülő igényekhez igazítása, az új technikai lehetőségek alkalmazhatóságának megteremtése;
- *d)* a rendszerbe állításra tervezett új informatikai és kommunikációs eszközök, rendszerek szolgáltatásainak, rendszerbe illeszthetőségének vizsgálata, döntés meghozatala az alkalmazhatóságukról, vagy alkalmazásuk kizárásáról, illetve az elavultak kivonásáról;
- *e)* a felhasználók részéről felmerült, az alapvető irodai informatikai és kommunikációs eszközökön és rendszereken túli igények elbírálása, a jogos igények lehetőség szerinti kielégítése, az adott szakterület vezetőjével egyeztetve javaslattétel az adott feladat ellátására alkalmas más eszköz, rendszer használatára;
- *f)* a felhasználók személyi számítógépeinek (asztali és hordozható gépek) felkészítése, a napi munkához szükséges programok, programrendszerek telepítése és konfigurálása, működési zavar, meghibásodás, rendellenes működés esetén a hibaelhárítás lehető leggyorsabb, de maximum 2 munkanapon belül történő megkezdése;
- *g)* az Egyetemen belüli levelezés során készült naplók, valamint az Egyetemről kifelé és az Egyetemre befelé irányuló levelezés, továbbá az internet használata során készült naplók 30 napig történő megőrzése;
- *h)* a kommunikációs rendszerek viszonylatában a jogszabályokban meghatározott nyilvántartások, naplók vezetése, amelyeket a jogszabályokban meghatározott esetekben és azon alapuló megkeresés alapján az illetékes hatóságoknak, szerveknek kiszolgáltat;
- *i)* a Hálózat és a szolgáltatások működéséhez, karbantartásához időközönként szükséges, előre tervezhető üzemszünetek, leállások 2 nappal a tervezett időpont előtt az Egyetem honlapján vagy e-mailben történő bejelentése;
- *j)* az általános informatikai ismereteken túli, az adott szolgáltatás igénybevételéhez szükséges ismeretek nyújtása.

(2) A biztonságos informatikai szolgáltatások nyújtása érdekében az INI jogosultságai
- *a)* a szolgáltatások körének, az egyes szolgáltatások igénybevételi feltételeinek meghatározása, melynek keretében a hálózati biztonság érdekében bármely szolgáltatás használatát felhasználói azonosításhoz (autentikációhoz) kötheti, a felhasználók körét szűkítheti, korlátozhatja;
- *b)* szankciók alkalmazása a biztonsági előírásokat megsértő felhasználókkal szemben

ba) a szabályok megszegése az Egyetem informatikai rendszerének, s így mások munkájának biztonságát is veszélyeztetheti, ezért az INI indokolt esetben azonnali kitiltást is alkalmazhat,

bb) a szankciók alkalmazása ellen a hallgató az INI igazgatójánál, a munkatárs a vezetőjénél élhet panasszal.

c) a Hálózat biztonsága érdekében a Hálózat használatának szabályait megsértő felhasználók hozzáférési jogosultságainak szűkítése vagy kizárása a szolgáltatások igénybevételéből;

d) a Hálózat biztonságos működését veszélyeztető vagy zavaró számítógépek, kommunikációs és más berendezések, eszközök Hálózatról történő előzetes értesítés nélküli leválasztása és intézkedés a zavar, illetve veszélyhelyzet megszüntetésére.

(3) A vezető jogai és kötelezettségei:

a) a vezető jogosult és köteles az irányítása alá tartozó munkatársak munkavégzéséhez szükséges infokommunikációs eszközök, valamint a használandó rendszerek és azokhoz szükséges jogosultságok körét meghatározni, továbbá az előzőek biztosításához szükséges engedélyezési eljárásokat kezdeményezni, illetve lefolytatni;

b) a vezető köteles az a) pontban foglalt, rendszer-, eszköz- és jogosultság-használatok indokoltságát kétévente legalább egyszer – az üzemeltetésben érintett szakterület által biztosított adatok alapján – írásban dokumentált módon felülvizsgálni és indokolt esetben a kiadott engedélyek módosítása vagy visszavonása érdekében szükséges intézkedéseket megtenni;

c) a vezető az informatikai biztonsági előírások megsértésnek észlelése esetén köteles:

ca) azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében,

cb indokolt esetben kezdeményezni a rendszer használatának felfüggesztését, illetve üzemszüneti eljárásrend bevezetését, amennyiben meghatározható rendszerre korlátozódik a biztonsági előírások megsértése,

cc) kivizsgáltatni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,

cd) a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni,

ce) tájékoztatni az INI igazgatóját.

d) a vezető jogosult az irányítása alá tartozó szervezeti egység tevékenységével kapcsolatos informatikai és/vagy informatikai biztonsági feltételrendszerre vagy azok szabályozására vonatkozó javaslatot tenni az INI igazgatója felé.

21. §

Az INI adatvédelmi kapcsolattartó jogai és kötelezettségei:

a) Amennyiben az Egyetem informatikai rendszerének fejlesztése, módosítása újabb informatikai alkalmazások fejlesztését, beszerzését indokolja, az adatvédelmi kapcsolattartó megvizsgálja, hogy az adatkezelés adatvédelmi szempontból a GDPR, illetve személyes adat kezelését előíró szabályzat hatálya alá esik-e, ennek eredményéről és az érintett személyes adatok köréről tájékoztatást ad az adatvédelmi tisztviselő részére, majd az adatvédelmi tisztviselő véleményét

követően tájékoztatja a munkatársat, hogy szükséges-e adatfeldolgozási szerződés megkötése.

b) A 9. § (4) bekezdésében meghatározott külső audittal kapcsolatban együttműködik az érintett munkatársakkal. A munkatárs a külső audit elrendelését megelőzően értesíti az adatvédelmi kapcsolattartót, aki tájékoztatja az adatvédelmi tisztviselőt az audit szükségességéről, illetve az érintett adatok köréről. Az adatvédelmi kapcsolattartó az adatvédelmi tisztviselő állásfoglalásáról tájékoztatja a munkatársat és amennyiben szükséges együttműködik az adatfeldolgozási szerződést előkészítése során az adatvédelmi tisztviselővel.

22. §

A Munkacsoport jogai és kötelezettségei:

a) amennyiben a felhasználó bejelentése alapján, vagy saját jogon tudomására jut, hogy az Egyetem által kezelt adatok köre biztonsági eseménynek van kitéve, értesíti az elektronikus információs rendszerek biztonságáért felelős személyt és az esetet haladéktalanul kivizsgálja;

b) amennyiben a biztonsági esemény személyes adatot érint, a kivizsgálás megkezdéséről haladéktalanul tájékoztatja az adatvédelmi tisztviselőt;

c) a vizsgálat eredményéről írásban tájékoztatja az adatvédelmi tisztviselőt, ha a biztonsági esemény személyes adatot érint.

23. §

A felhasználó jogai és kötelezettségei:

a) A felhasználó jogosult a munkavégzéshez szükséges infokommunikációs eszközöket használni, a használatukhoz szükséges ismereteket dokumentáció vagy oktatás formájában megkapni.

b) A munkavégzéshez szükségesnek ítélt eszközök, szoftverek beszerzését, telepítését igényelni (az igény jogosságát a szakterület vezetőjével együttműködve az INI bírálja el).

c) A felhasználó a rendelkezésére bocsátott infokommunikációs eszközöket csak az Egyetem céljaival, feladataival kapcsolatos, a munkaköri feladatai ellátásához szükséges tevékenység céljára, rendeltetésszerűen, a számára megállapított jogosultságok keretein belül, rendeltetésszerűen használhatja.

d) A Hálózatra bármilyen berendezést (különösen: számítógépeket, perifériákat – nyomtató, scanner külső adattárolók – fax, okostelefon, stb.) csak az INI engedélyével szabad csatlakoztatni. Ha az eszköz adattárolásra is alkalmas, akkor a csatlakoztatás után vírusellenőrzést kell végrehajtani, illetve az adatok tárolására vonatkozó jelen és más vonatkozó egyetemi szabályzatok és előírások betartására különös figyelmet kell fordítani

e) A felhasználó köteles a használatra átvett informatikai eszközöket az elvárható gondossággal kezelni és a károsodásoktól védeni.

f) A felhasználó személyes anyagi felelősséggel tartozik az általa szándékosan vagy gondatlanságból (pl. nem rendeltetésszerű használattal) az infokommunikációs eszközökben okozott bizonyított károkért.

g) A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tevékenységért, tranzakcióért a bejelentkezéstől a kijelentkezésig a felhasználó felelős. Ez a felelősség akkor is fennáll, ha a tevékenységet,

tranzakciót harmadik személy hajtotta végre, amennyiben erre a Szabályzat előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.

h) A munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, jelszavas képernyőkímélővel védeni, illetve ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni, vagy azt kikapcsolni, amennyiben azt felügyelet nélkül hagyja. A munkaállomást a munkaidő végén vagy a munkavégzés befejezésekor – eltérő rendelkezés hiányában – ki kell kapcsolni.

i) Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, a felhasználói fiókból és az azonosított kapcsolatból is kijelentkezett.

j) Azt a munkaállomást, infokommunikációs eszközt, amelybe privilegizált rendszeradminisztrátor jogosultsággal jelentkeztek be, személyes felügyelet nélkül hagyni tilos.

k) A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott dokumentumhoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott dokumentumot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

l) A felhasználó a rendelkezésére bocsátott mobil infokommunikációs eszközöket és adathordozókat köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

m) A felhasználó köteles a 25. §-ban meghatározott informatikai biztonsági eseményről vagy annak bekövetkezési lehetőségéről értesíteni közvetlen vezetőjét és a Munkacsoportot. A felhasználó köteles a saját feladatkörében nem megoldható informatikai biztonsági problémáról, hiányosságról értesíteni közvetlen vezetőjét és a feladatkörrel rendelkező, kijelölt Munkacsoportot, és közreműködni a szükséges intézkedések végrehajtásában.

n) A felhasználó köteles meghibásodás, üzemzavar észlelésekor, vírusfertőzés (vagy annak gyanúja) esetén haladéktalanul értesíteni az INI-t, a számítógép további használatát az INI munkatársainak intézkedéséig felfüggeszteni. A hibaelhárítás folyamán az INI szakembereivel együttműködni, számukra a szükséges információkat megadni.

o) Az m) és n) pontokban meghatározott események tudomásszerzésekor a Munkacsoport haladéktalanul kivizsgálja az esetet és az eredményről tájékoztatást küld az adatvédelmi tisztviselőnek, kivéve azon meghibásodási eseteket, amelyeknél adatvédelmi incidens egyértelműen nem történt.

A meg nem engedett tevékenységek szankciói
24. §

Jelen Szabályzat megsértésének gyanúja esetén a cselekményt ki kell vizsgálni, és a vizsgálatra a rektor által megbízott legalább három tagú felelős (kivizsgáló) bizottságnak javaslatot kell tennie a megbízónak a szükséges intézkedésekre, amelyekre a következők az irányadók:

a) a Szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni;

b) a Szabályzat ismételt megszegése szándékos elkövetésnek minősül;

c) a Szabályzat szándékos megsértése esetén az elkövető a Hálózat használatából ideiglenesen vagy véglegesen kizárható és az eset súlyosságától függően eljárás lefolytatása kezdeményezhető ellene azzal, hogy az Egyetem informatikai Hálózatának szolgáltatásait csak az eljárás lefolytatása után és annak eredményétől függően veheti igénybe.

d) a szándékos elkövető – a fentieken túl, amennyiben kimutatható anyagi kár is keletkezett – köteles megtéríteni az általa okozott károkat a vonatkozó jogszabályok és más közjogi szervezetszabályozó eszközök előírásai szerint;

e) ha az elkövetett cselekmény kimeríti a Btk. valamely törvényi tényállását, akkor a vizsgálatért a kivizsgáló bizottság javaslatára a rektorköteles az elkövető felelősségre vonását kezdeményezni.

A felhasználó által jelentendő biztonsági esemény
25. §

(1) A felhasználó köteles az általa észlelt informatikai biztonsági eseményről vagy annak bekövetkezési lehetőségéről azonnal értesíteni közvetlen vezetőjét és az INI Service Desk szolgálatát.

(2) A felhasználó köteles az informatikai biztonsági eseményt előidéző okokat megszüntetni, amennyiben erre saját hatáskörben vagy az eseményt előidéző személy bevonásával lehetősége van. Amennyiben ez nem lehetséges vagy nem járt sikerrel, a biztonsági esemény kezelésében köteles közreműködni, amennyiben erre a biztonsági esemény kezeléséért felelős személytől felkérést, utasítást kap.

(3) A felhasználó a fentiek szerint köteles eljárni, amennyiben az alábbi körbe tartozó informatikai biztonsági eseményt észlel, vagy ilyenre gyanakszik:

a) a felhasználói azonosítóval való visszaélés, illetéktelen rendszer- vagy adathozzáférés, bármely, a felhasználó által használt szolgáltatás, rendszer, infokommunikációs eszköz tekintetében (pl. elektronikus levelezés, szakrendszer stb.),

b) adathalász tevékenység, amely a felhasználó személyes adatainak vagy intézményi hozzáféréseinek, illetve az intézményt érintő – nem publikus – információk megszerzésére irányul (pl. adathalász oldalak, kéretlen levelek vagy közvetlen telefonhívások, amelyek személyes vagy munkahelyi információk megszerzésére irányulnak),

c) rosszindulatú szoftverek (vírusok, trójai programok stb.) jelenléte a felhasználó által használt rendszeren, infokommunikációs eszközön,

d) adatszivárgás, ami megvalósulhat az érintett szervezet adatvagyonát képező nem közérdekű adatok szándékos vagy véletlen továbbításával, kiszivárogtatásával azok megismerésére nem jogosult szervezetek, személyek vagy az adatok bizalmasságának megőrzése szempontjából megbízhatatlan rendszerek felé,

e) felhasználó használatában lévő informatikai eszköz elvesztése, ezek megbontására utaló jelek.

(4) A felhasználó köteles az INI Service Desk szolgálatának bejelenteni, ha bármilyen megfigyelhető vagy valószínűsíthető információbiztonsági gyengeséget észlel a rendszerekben vagy szolgáltatásokban.

Az informatikus munkakört ellátó munkatárs jogai és kötelezettségei
26. §

(1) Az informatikus munkakört, szerepkört, feladatkört ellátó munkatárs a felhasználói jogosultságokon túlmutató többletjogosultságait csak a jogszabályokkal és a belső szabályzatokkal összhangban, rendeltetésszerűen, a munkaköri leírásában foglalt feladatok ellátásához használhatja.

(2) A rendszergazda részletes felelősségét és hatáskörét a munkaköri leírása tartalmazza, amely magába foglalja az alábbiakat:

a) az egyetemi Hálózat biztonsági kockázatának minimalizálása;
b) az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismerése és jelentése;
c) az informatikai szabályok betartása és betartatása;
d) a hálózati rendszergazdák feladata a felelősségi és hatáskörükbe tartozó szerverek, valamint a hálózati aktív eszközök hardver és szoftver felügyelete, napi működésének biztosítása;
e) a szervezeti rendszergazdák feladata az egyes egyetemi szervezetek kezelésében lévő, az INI igazgató engedélyével működő, hálózati szolgáltatást nyújtó számítógépek üzemeltetése, az általuk üzemeltetett szerverek működésének biztosítása, valamint a hálózati rendszergazdák által megszabott üzemeltetési feltételek betartása, betartatása azzal, hogy a szervezeti rendszergazdákat a megfelelő szakismerettel rendelkező személyek közül, az adott egyetemi szervezet vezetőjének javaslata alapján az INI igazgatója jelöli ki.
f) a felügyelt szerverek, informatikai rendszerek katasztrófa és mentési terveinek elkészítése, az adatállományok rendszeres mentése, az esetlegesen bekövetkező katasztrófák következményeinek felszámolásával kapcsolatos tevékenységek begyakorlása.

Informatikai biztonságot érintő események kezelése
27. §

(1) Az INI informatikai rendszerrel támogatott hibajegy kezelő rendszert üzemeltet az események kezelésére. A felhasználói és üzemeltetői bejelentésének fogadását az Egyetem egykapusan végzi, azaz az incidenst csak a https://servicedesk.uni-nke.hu portál felületen lehet bejelenteni.

(2) A bejelentés utáni folyamatot elektronikus hibajegy kezelő és feladat támogató rendszer segíti.

(3) Az informatikai biztonságot érintő események saját észlelése vagy a felhasználói bejelentés után munkaidőben 5 percen belül, munkaidőn túl 10 percen belül az INI Service Desk hibajegyet nyit és megkezdi a feldolgozást. A bejelentésről egyedi azonosítószám kerül rögzítésre. Az esemény bekövetkezéséről azonnal értesíteni kell az INI igazgatót.

VIII. FEJEZET
ADMINISZTRATÍV BIZTONSÁGI KÖVETELMÉNYEK
Rendszerek dokumentálása
28. §

(1) A rendszerek teljes életciklusát dokumentálni kell, így a tervezés (követelmény-meghatározás), a fejlesztés és a továbbfejlesztés vagy a beszerzés, a tesztelés és az ellenőrzés, az üzemeltetés, a fenntartás és a karbantartás, valamint a megszüntetés (kivonás, archiválás, megsemmisítés) fázisait is.

(2) A dokumentáció teljességéért és naprakészségéért (folyamatos aktualizálásáért) a fejlesztő, a rendszer üzemeltetésének megkezdésétől az üzemeltető szervezeti egység vezetője felel.

(3) A rendszer dokumentációja akkor teljes, ha tartalmazza az üzleti (funkcionális), az informatikai és az informatikai biztonsági szempontból releváns valamennyi adatot.

(4) Az egyes rendszerek esetében elvárt dokumentumok körét és mélységét a rendszer tervezésekor kell meghatározni, amelyeket a rendszer teljes életciklusa alatt folyamatosan frissíteni szükséges.

(5) A dokumentáció tartalmazza a rendszer által megvalósítandó üzleti funkciókban résztvevő rendszerelemek meghatározását, az üzleti funkció megvalósításának módját mind fizikai, mind logikai szempontból.

(6) A dokumentáció tartalmazza a rendszerben alkalmazott biztonsági megoldásokat, beleértve a rendszer egy esetleges részleges vagy teljes körű meghibásodása vagy megsemmisülése esetére kidolgozott eljárásrendet.

(7) A rendszerek dokumentációjának őrzéséről, az arra jogosultak számára hozzáférhetővé tételéről, továbbá folyamatos aktualizálásáról a szakmai felügyeletet ellátó szervezeti egység bevonásával az üzemeltetésért felelős szervezeti egység gondoskodik.

(8) A rendszer üzemeltetéséhez és használatához szükséges dokumentációt – így különösen a rendszerüzemeltetési szabályzatot, az üzemeltetési leírást és a felhasználói kézikönyvet vagy felhasználói leírást – a rendszer üzemeltetésének megkezdése előtt el kell készíteni és az érintettek számára – jellemzően elektronikus úton – hozzáférhetővé kell tenni.

Szolgáltatások, rendszerek és rendszerelemek nyilvántartása
29. §

(1) Az Egyetem által nyújtott informatikai szolgáltatásokat nyilván kell tartani. A szolgáltatás-nyilvántartás kialakításáért és vezetéséért (pontosságáért és naprakészségéért) az INI igazgatója a felelős.

(2) A szolgáltatás-nyilvántartás alapja az Egyetem Szolgáltatási katalógusa, amely tartalmazza:

a) a szolgáltatás összefoglaló meghatározását,

b) a szolgáltatás leírását (a szolgáltatás részei, szintjei, egyéb jellemzői, feltételei, kivételek stb.).

(3) Az Egyetem működése során használt, továbbá az általa nyújtott szolgáltatásokban érintett és a birtokában és/vagy felügyelete alatt álló rendszereket és rendszerelemeket, valamint licenceket nyilván kell tartani.
(4) Az INI rendszer-nyilvántartást vezet. A rendszer-nyilvántartás a rendszerek alapadatait tartalmazza, az adatköröket az üzemeltetési központ szakmai igényei szerint kell kialakítani.

(5) A licencnyilvántartás kialakításáért és vezetéséért (hitelességéért, pontosságáért és naprakészségéért) a Rendszerüzemeltetési Iroda vezetője felelős.

(6) Az infokommunikációs eszközök és anyagok nyilvántartásával és mozgatásával kapcsolatos részletes előírásokat az Egyetem leltározási és leltárkészítési, valamint a telekommunikációs szabályzatai tartalmazzák.

IX. FEJEZET
ÜZLETMENET-FOLYTONOSSÁG ÉS SZOLGÁLTATÁS-FOLYTONOSSÁG BIZTOSÍTÁSA
Szolgáltatás-folytonossági tervezés
30. §

(1) A rendszer üzemeltetéséért felelős a rendszerre vonatkozó szolgáltatásfolytonossági tervet (ITSCP) készít, amelyben meghatározza:
- *a)* a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket,
- *b)* a folyamatos működéshez szükséges infokommunikációs és környezeti képességek biztosításához szükséges kapacitást,
- *c)* az alapfeladatokat biztosító szolgáltatásokat és alapfunkciókat,
- *d)* az alapfunkciókat támogató kritikus rendszerelemeket,
- *e)* a vészhelyzeti követelményeket, szerepköröket, felelősségeket, felelősöket,
- *f)* az alapfunkciók, illetve az összes funkció újrakezdésének időpontját az ITSCP aktiválását követően,
- *g)* a helyreállítási feladatokat, prioritásokat, mértékeket,
- *h)* a teljes rendszer helyreállításának tervét (DRP) úgy, hogy az eredeti biztonsági megoldások is helyreállításra kerüljenek.

(2) Az ITSCP-t
- *a)* úgy kell elkészíteni, hogy a folyamatos működés tervezésére vonatkozó tevékenységeket összehangolják a biztonsági események kezelésével,
- *b)* a készítő szervezeti egységnek, ha a rendszer üzemeltetési körülményeiben jelentős változás következett be, a változást követő 30 napon belül – dokumentáltan – felül kell vizsgálnia és szükség szerint aktualizálnia,
- *c)* a rendszer folyamatos működésében érintett szervezeti egységek számára hozzáférhetővé kell tenni, beleértve az aktualizálásokat is,
- *d)* az arra nem jogosultak számára tilos hozzáférhetővé tenni.

Tartalék helyszínek és szolgáltatások
31. §

(1) A folyamatos működés biztosítása érdekében az Egyetem által üzemeltetett rendszerek esetében infrastruktúra szinten két, azonos funkcionalitású adatközpont kialakításról kell gondoskodni. A két csomópontos kialakítást földrajzilag különböző elhelyezkedésű objektumokban kell megvalósítani (ezt nevezik geo-redundáns elhelyezésnek). Ennek célja a helyi infrastrukturális hibáknak (pl.: áramszünet stb.) és vis major eseményeknek (villámcsapás, tűz, árvíz, stb.) az informatikai szolgáltatás minőségére és biztonságára gyakorolt hatásainak csökkentése.

(2) Az egyes rendszerek esetében az elsődleges és a másodlagos csomópont kijelöléséről az üzemeltetésért felelős dönt.

(3) Az egyes rendszerek kialakításának megfelelően a két csomópontos működés megvalósulhat aktív-aktív módon is. Ebben az esetben a méretezést úgy kell megvalósítani, hogy az egyes csomópontok önállóan képesek legyenek teljesíteni a teljes rendszerre vonatkozóan meghatározott kapacitásigény kiszolgálását.

Mentés és archiválás
32. §

(1) A rendszerekben kezelt, feldolgozott, tárolt adatok rendelkezésre állását rendszeres és indokolt esetben soron kívüli mentéssel kell biztosítani.

(2) Az Egyetem működése során használt rendszerek esetében naponta egy automatikus mentést kell végrehajtani. A mentés eredményét az adott rendszer tárolja, a két site-os rendszerekben a mentés eredményét a túloldali site-ra replikálni kell.

(3) Meghatározott adatbázisok esetében a mentési gyakoriság 2-6 óra.

(4) Az érintett rendszerek esetében legalább havonta egy rendszer szintű teljes mentést kell készíteni, amelynek elkülönített és biztonságos off-site tárolásáról az INI gondoskodik. A teljes mentések elkülönített off-site megőrzéséről legfeljebb 30 napig kell gondoskodni, melynél hosszabb időt egyetemi szabályzat megállapíthat.

(5) A rendszerekben kezelt, feldolgozott, tárolt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során már nem szükséges, azonban őrzésük indokolt, archiválni kell.

(6) Az (5) bekezdésben meghatározott adatállományt – amennyiben személyes adatot is tartalmaz – az őrzési idő elteltével törölni kell.

(7) A mentési és archiválási eljárásokat, a vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy azok

a) a szakmai bevált gyakorlatokon alapuljanak, kielégítő biztonságot adjanak az arányosság elvének figyelembe vételével,
b) a rendszereket érintő, jelentős meghibásodások és megsemmisülések hatásait hatékonyan kivédhetővé tegyék,
c) biztosítsák az adatvesztések elkerülését vagy minimalizálását.

(8) A mentési tervet az INI alakítja ki a jogszabályi, belső-, és külső előírások, valamint a technológiai lehetőségek figyelembe vételével.

(9) Az egyes rendszerek esetében a speciális előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

(10) A rendszerekben kezelt, a felhasználók számára a munkavégzéshez már nem szükséges adatállományokat törölni kell. A törlés megtörténtéről jegyzőkönyvet kell felvenni.

X. FEJEZET
FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK
A Hálózat
33. §

(1) Az Egyetem Hálózata több telephelyes, több településre kiterjedő hálózat. A Hálózat logikai felépítése az alábbi:

a) Az Egyetem Hálózata tűzfalakkal védett, logikailag zónákra osztott. Telephelyenként külön-külön zónákban működnek az oktatói-dolgozói, tantermi illetve a kollégiumokban működő gépek, valamint a több irányba szolgáltatást nyújtó szerver számítógépek. A hálózati működés biztosításához, illetve speciális feladatokhoz további zónák is kialakításra kerülhetnek.

b) Az egyes telephelyek logikai felépítése hasonló, a telephelyek közötti forgalom tűzfalakkal szabályozott, a definiált informatikai szolgáltatások elérhetősége minden telephely esetében biztosított.

c) Az egyes számítógépek illetve szolgáltatások különböző zónákba történő besorolását a hálózati rendszergazdák javaslatainak figyelembe vételével az INI igazgatója határozza meg.

(2) A Hálózat mindenkori műszaki paramétereit külön dokumentáció tartalmazza.

(3) Kizárólag az INI jogosult a Hálózat megváltoztatására (bővítésére, átalakítására, kiépítésére). A Hálózatot, a lehetőségeket figyelembe véve az INI az igényeknek megfelelően folyamatosan bővíti, karbantartja. Hálózat vagy hálózatrész építése, módosítása, valamint az Egyetem rendszerén kívüli szolgáltatásokhoz, hálózatokhoz állandó kapcsolat (különösen site-to-site VPN) létesítése külső erőforrások (különösen: pályázat, és más jellegű támogatások) bevonása esetében is csak az INI igazgatójának jóváhagyásával történhet. Szigorúan tilos a felhasználó saját vezeték nélküli illetve aktív hálózati eszközeinek bekötése a hálózatba.

(4) Hálózati aktív eszközöket (repeater, HUB, switch, router, tűzfal) csak az INI szakemberei vagy megbízottjaik csatlakoztathatnak vagy köthetnek le a Hálózatról. Az aktív eszközök kapcsolatainak megbontására, az eszközök bármilyen eszközzel történő átkonfigurálására csak az INI szakemberei vagy megbízottjaik jogosultak. Az INI szakembere és megbízottja olyan személy vagy szervezet lehet, akit az INI szakmailag kellő felkészültséggel rendelkezőnek tart a művelet adatvédelmi szempontból történő biztonságos elvégzésére.

(5) Az Egyetem Hálózatának elsődleges protokollja az IP protokoll, támogatottak az IP feletti protokollok.

(6) Az INI az egyes protokollok, portok, illetve az ezeket használó alkalmazások használatát a működési stabilitás és az adatbiztonság érdekében időlegesen vagy véglegesen, VLAN-onként, telephelyenként vagy az Egyetem teljes Hálózatára kiterjedő hatállyal korlátozhatja vagy megtilthatja.

A rendszerek, rendszerelemek, infokommunikációs eszközök telepítése és tárolása
34. §

(1) A rendszereket, rendszerelemeket, infokommunikációs eszközöket úgy kell telepíteni és tárolni, hogy

a) a lehető legkisebb mértékre csökkentsék a fizikai és környezeti veszélyekből adódó lehetséges károkat,
b) azokhoz a jogosult munkatársakon és az Egyetemmel polgári jogi jogviszonyban álló személyeken kívül más személy hozzáférése – jogosulatlan hozzáférés – kizárt (a lehető legkisebb mértékűre csökkentett) legyen.

(2) A környezeti feltételeket a befogadó helyiségek rendeltetése, a telepítési környezetek alapján az alábbiak szerint kell meghatározni:

a) irodai környezet (jellemzően a felhasználói és az általános informatikai tevékenységet támogató munkaállomások befogadására szolgáló helyiségek),
b) kiemelt informatikai munkaterület (speciális, az irodai környezet védelmi igényét meghaladó informatikai eszközök befogadására szolgáló helyiségek, pl. fejlesztői körlet, informatikai eszközök raktára stb.),
c) gépterem (az informatikai erőforrásokat koncentráltan tartalmazó helyiségek, pl. a rendszerek, szolgáltatások központi üzemeltetését és irányítását végző infokommunikációs eszközöket befogadó létesítmények, csomópontok, adatközpontok, számítóközpontok, szerverszobák, kommunikációs elosztóhelyiségek stb.).

A géptermek és szerverhelyiségek kialakítása
35. §

(1) Az Egyetem által működtetett géptermekre vonatkozó előírásokat az NKE Gépterem használati Rend tartalmazza, így különösen az alábbi szabályokat:

a) belépés és beléptetés rendje,
b) fizikai behatolás-riasztások és felügyeleti berendezések kezelése,
c) áramellátás, rövid távú, szünetmentes és hosszú távú, tartalék áramellátás, továbbá kábelezés megvalósítási módja,
d) vészhelyzeti kikapcsolás megvalósítási módja,
e) automatikus vészvilágítási rendszer alkalmazása és karbantartása,
f) tűzvédelem,
g) hőmérséklet- és páratartalom biztosítása,
h) csővezeték-rongálódásból származó károkkal szembeni védelem,
i) a helyiségben végzendő javító, karbantartó, takarító stb. tevékenységek végzésének rendje.

(2) Az Egyetem ellenkező rendelkezés hiányában nem támogatja az általa működtetett géptermekbe nem Egyetem által üzemeltetett eszközök bevitelét, működését.

Kritikus adatokat tartalmazó számítógépek használata
36. §

Az adatvédelmi szempontból kritikus adatokat (különösen: személyügyi, pénzügyi, ügyviteli adatokat, információkat) tároló számítógépek védelmére fokozott figyelmet kell fordítani. Zárt, teljes körű, folytonos és kockázatokkal arányos, adatvédelmet és biztonságot kell biztosítani. Ezen gépek körét az érintett szervezetek vezetői határozzák meg. Az igényelt, internetkapcsolat nélküli biztonságos belső hálózati kapcsolat biztosítása az INI feladata.

Szerverek üzemeltetése
37. §

(1) Az Egyetemen kívülre, az Egyetem egésze vagy egy-egy kampusza számára szolgáltatást nyújtó szerverek felügyelete – beleértve az operációs rendszereik karbantartását, frissítését is – az INI által kijelölt egyetemi rendszergazdák, központi adminisztrátorok és az együttműködésre szerződött vagy kijelölt személyek feladata.

(2) Az INI által üzemeltetett számítógépeken kívül szerverek, informatikai szolgáltatások elindítása, ilyen szolgáltatást nyújtó számítógépek Hálózatra kapcsolása csak az INI igazgatójával történt egyeztetés után történhet.

XI. FEJEZET
LOGIKAI BIZTONSÁGI KÖVETELMÉNYEK

38. §

A rendszerre vonatkozó informatikai védelmi megoldásokat új rendszer esetében a fejlesztő, már működő rendszer esetében az üzemeltető tervezi meg és gondoskodik azok megvalósításáról, beleértve a szükségessé váló korszerűsítéseket, módosításokat is.

XII. FEJEZET
HOZZÁFÉRÉS A RENDSZEREKHEZ

A felhasználó azonosítása és feljogosítása a rendszer használatára
39. §

(1) A felhasználó a rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.

(2) A rendszer használata során a felhasználó egyedi azonosítását folyamatosan biztosítani kell. Minden felhasználót kizárólagos személyi használatú azonosítóval kell ellátni, amelyhez egyedi jelszót kell rendelni.

(3) A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:

a) **Tilos** a felhasználóra jellemző, könnyen kitalálható (különösen: vezetéknév, keresztnév, saját gyermekek, ismert kedvenc személy, kedvenc háziállatok, stb.) jelszavakat választani.

b) **Tilos** a login nevet jelszóként használni.
c) **Tilos** azonos vagy az abc-ben, a billentyűzeten egymást követő számokból vagy betűkből álló jelszót használni.
d) A jelszó hossza nem lehet rövidebb nyolc karakternél, de 20 karakter maximumú lehet), tartalmaznia kell legalább kettő (maximum 18) számjegyet, valamint legalább egy nagybetűt, és minimum egy (maximum 17) kisbetűt. A jelszó ékezetes betűt nem tartalmazhat. Jelszavak választásakor javasolt a számok, a kis- és nagybetűk keverése, a könnyebb megjegyezhetőség érdekében rövid jelmondatok szóköz nélküli, és a szavak nem szótári alakban történő használata stb.
e) **Tilos** a jelszót nyilvános helyen kiírva tartani (különösen: monitorra ragasztva).
f) A hálózati belépésre jogosító jelszót kötelező – az egyéb jelszavakat ajánlott rendszeresen, de legalább – 180 naponta újracserélni.

(4) A felhasználók a Hálózathoz, rendszerekhez történő hozzáférést biztosító jelszavakat – első alkalommal – az illetékes rendszergazdáktól lezárt borítékban kapják meg, vagy a felügyeletükben a felhasználók saját maguknak állítják be. A borítékban kiadott jelszavakat az első belépést követően azonnal módosítani kell.

(5) Az elfelejtett, lejárt jelszavak helyett új jelszavak kiadása csak személyesen, az illetékes rendszergazdánál az első alkalommal történt jelszavak kiadásához hasonlóan történik.

(6) Az Egyetem Hálózatához történő hozzáférés – jelszó igénylés – jogosultságának ellenőrzése érdekében a rendszergazda kérheti a felhasználó egyetemi belépőkártyáját, vagy az érvényes „személyazonosításra alkalmas hatósági igazolványát” (személyazonosító igazolványát, vagy útlevelét, vagy kártyaformátumú vezetői engedélyét).

40. §

(1) Az Egyetem az azonosítási, autentikációs és jogosultságkezelési feladatok támogatására központi címtárat alkalmaz, amelynek használatát új rendszerek kialakításakor lehetőség szerint tervezni kell.

(2) Az azonosítás, az autentikáció és a jogosultságkezelés folyamatát az egyes rendszerek esetében a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

(3) A jelszó megváltoztatása kötelező:
a) a felhasználói azonosító rendszerbe történő felvételét követő első bejelentkezéskor,
b) az üzemeltető munkatársa általi újbóli jelszóbeállítást követően,
c) ha a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett,
d) az érvényességi idő lejártakor.

(4) Amennyiben a felhasználó elfelejtette a jelszavát, úgy a rendszert üzemeltető szervezeti egységtől kell jelszócserét kérni.

(5) A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelen személy általi megismerését kizárni. Amennyiben a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett, erről a tényről a felhasználó köteles tájékoztatni a közvetlen vezetőjét, aki gondoskodik az elektronikus információs rendszerek biztonságáért felelős személy tájékoztatásáról. A szükséges intézkedések megtételéről a közvetlen vezető és az INI együttesen, feladatkörüknek megfelelően gondoskodnak.

(6) Az INI és más szervezetek informatikusai, a rendszergazdák sosem kérik telefonon vagy e-mailen keresztül megadni a jelszavakat, legfeljebb csak a felhasználó által az azonnali módosítását. Ha valaki ezt kéri, ez gyanús és értesíteni kell az INI-t.

(7) A jelszócseréről a felhasználó köteles azonnal gondoskodni; amennyiben a jelszócserét nem tudja önállóan végrehajtani, az INI Service Desk szolgálattól kell jelszócserét kérni.

(8) Új munkatárs belépésekor vagy új eszköz (rendszer) első használatba vételekor a felhasználó egy központilag generált alapjelszót kap, amelyet az átvételt követő első bejelentkezéskor köteles megváltoztatni (amikor ez technikailag megoldható, az eszköz vagy a rendszer ki is kényszeríti).

41. §

(1) A jelszóképzésre és a jelszóvédelemre vonatkozó előírások a privilegizált felhasználók esetében is értelemszerűen alkalmazandók.

(2) Hibás jelszóval történő többszöri bejelentkezési kísérletek esetén az adott felhasználói fiók zárolásra kerül az alábbiak szerint:

a) fiók zárolási határértéke: 10 próbálkozás,
b) fiók zárolási ideje: 15 perc,
c) fiók zárolásának feloldása: 15 percet követően.

(3) Amennyiben egyes szoftverek működéséhez egyedi felhasználói azonosító – service account – használata szükséges, azt az üzemeltetési szakterület munkatársai a telepítés során állítják be. Az alkalmazások működését a jelszavak kötelező megváltoztatása megakadályozza, ezért a service account-ok mentesülnek a kötelező jelszóváltoztatás alól, viszont csak az adott program futtatásához szabad felhasználni.

(4) Egyes rendszerek, felhasználók, további hozzáférési módok esetében a jelszavas azonosítást birtoklás vagy tulajdonság alapú azonosítás egészíti ki.

Távoli hozzáférés
42. §

(1) Az INI a munkahelyi vezetők javaslatai alapján lehetővé teszi a kijelölt felhasználók részére az egyetemi Hálózat bizonyos részeinek távoli elérését. A távoli munkavégzés során is be kell tartani a biztonsági rendszabályokat, különös tekintettel az illetéktelen hozzáférés megakadályozására. A távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó a Hálózaton titkosított formában haladjon, valamint az adatforgalmat is titkosítani kell.

(2) Az Egyetem Hálózatára a távoli munkavégzés során VPN segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme, az illetéktelen hozzáférés megakadályozása a felhasználó kötelessége.

(3) Távoli hozzáférés igénylésre a jogosultságigénylésre vonatkozó előírások irányadók azzal, hogy az igényléshez a közvetlen vezető engedélyén túl az INI igazgatójának jóváhagyása is szükséges. Az igénylés során minden esetben pontosan fel kell tüntetni az elérni kívánt rendszer, szolgáltatás adatait.
(4) A fejlesztői célú távoli hozzáférés alapesetben nem engedélyezett. Az előírás alóli kivételt indokolt esetben, meghatározott időtartamra az INI igazgatója engedélyezi.

(5) Az azonosításhoz és feljogosításhoz biztosított (fizikai) eszközök védelmére a jelszóvédelemre, a távoli elérés igénylésére a jogosultságigénylésre, a külső munkatársak számára biztosított távoli elérésekre a külső munkatársakra vonatkozó előírások értelemszerűen irányadók.

(6) Az egyes rendszerek esetében a speciális előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

(7) A távoli hozzáféréssel kapcsolatos működési és felhasználói események automatikus naplózását biztosítani kell, a naplóadatokat 3 hónapig meg kell őrizni. A 3 hónap elteltével az adatokat törölni kell.

Jogosultságkezelés
43. §

(1) A munkatárs részére csak a munkaköre ellátásához szükséges és elégséges jogosultságok adhatók ki. A rendelkezés megtartásáért a munkatárs közvetlen vezetője a felelős.

(2) Az Egyetemmel polgári jogi jogviszonyban álló munkatárs jogosultságait a munkatársat foglalkoztató szervezeti egység vezetője engedélyezheti és igényelheti, továbbá köteles rendelkezni a jogosultság visszavonásáról is.

(3) A jogosultságokat úgy kell kialakítani, hogy megkülönböztethetők legyenek a felhasználói és a privilegizált felhasználói jogosultságok, jogosultságcsoportok.

(4) A jogosultságokat felhasználói csoportokhoz kell rendelni; a munkatársak felhasználói csoportbeli tagsága biztosítja a jogosultságok használatát.

(5) A munkatárs a számára engedélyezett szolgáltatásokat, alkalmazásokat, szoftvereket mások számára semmilyen módon nem teheti hozzáférhetővé, illetve az infokommunikációs eszközöket nem használhatja más felhasználó nevében (indokolt esetben betekintési jogot adhat az általa kezelt adatokba, pl. postafiókjába). A felhasználó helyettesítése esetén a helyettes bejelentkezése saját néven, saját – szükség esetén határozott időtartamra igényelt külön – jogosultsággal történhet.

(6) Amennyiben a munkatárs jogviszonya megszűnik, továbbá ha a jogviszonyában olyan változás következik be, amely miatt a munkavégzéséhez a korábban igényelt jogosultságok nem szükségesek, amennyiben a jogosultságok visszavonása nem történik

meg informatikai rendszer által támogatottan automatikusan, a munkatárs közvetlen vezetője köteles a jogosultságok visszavonását kezdeményezni.

(7) A jogosultságot a munkatárs számára a közvetlen vezetője engedélyezheti vagy vonhatja vissza. A jogosultságigénylést a rendszer működtetéséért felelős szervezeti egység, az adatgazda, valamint a licencgazdálkodásért felelős szervezeti egység vezetője ellenjegyzi, a jogosultság csak ezt követően állítható be.
(8) A jogosultság beállításával, törlésével és nyilvántartásával kapcsolatos feladatokat a jogosultság-adminisztrátorai látják el.

(9) Biztonsági okokból és a későbbi visszakereshetőség, elemzések elvégzése érdekében – a szervereken – az egyetemi Hálózatba történő sikeres és sikertelen belépési kísérletek is rögzítésre, naplózásra kerülnek.

(10) Ha jogosulatlan hozzáférés történt, vagy a jogosulatlan hozzáférés gyanúja merül fel, a jelszót azonnal meg kell változtatni.

(11) Jogosultsági szint összefoglaló táblázat

Szint	Jogosultak	Jogok	Felelős
Külső	Vendégoktató, kutató, tanfolyami, rendezvény résztvevő	Internet elérés, WiFi használat	Szervezeti egység vezetője
Alap	Egyetem hallgatói, dolgozói	Egyéni azonosítás alapján lehetővé válik az oktatáshoz, tanuláshoz, munkához szükséges adatok, programok, levelezés, valamint az Internet elérése.	Karok és szervezeti egységek vezetői
Adminisztrátor	Adminisztrációval kapcsolatos munkakörök	Alapszint+hozzáférés az adminisztrációs, dokumentációs rendszerekhez, szervezeti egység közös lemezterületéhez.	Szervezeti egység vezetője
Oktató, kutató	Az Egyetem oktatói, kutatói	Alapszint+hozzáférés az oktatói, kutatói rendszerekhez, a szervezeti egység közös lemezterületéhez, a hallgatókkal kapcsolatos adminisztrációs adatokhoz.	Karok és szervezeti egységek vezetői
Tanulmányi	Oktatási és Tanulmányi Iroda, Kari Tanulmányi Osztályok	Alapszint+teljes körű hozzáférés a Neptun rendszer adminisztratív moduljaihoz.	Oktatási ügyekért felelős rektorhelyettes, illetékes tanulmányi vezető
Gazdasági	Gazdasági Hivatal dolgozói a	Alapszint+hozzáférés a gazdálkodással és a	Gazdasági Főigazgató

	jogosultsági szintnek megfelelően	dolgozókkal kapcsolatos rendszerekhez.	
Humánpolitikai	Humán Iroda dolgozói a jogosultsági szintnek megfelelően	Alapszint+hozzáférés a dolgozókkal kapcsolatos rendszerekhez.	Főtitkár
Rendszer-gazda (hálózati, szervezeti)	INI, egyetemi szervezetek rendszergazdái	Korlátlan jog a rendszergazda által felügyelt rendszerekhez (különösen: hálózat, storage, szerverek, adatbázisok, mentési rendszer, egyetemi szervezet által felügyelt szerver).	INI Igazgatója
Alkalmazás rendszergazda	Egy adott alkalmazás informatikai rendszergazda	Korlátlan jog az adott alkalmazáshoz. (különösen: AVIR, Forrás SQL, Neptun, NEO).	INI Igazgatója, egyetemi szervezeti egység vezetője

44. §

(1) A jogosultságkezelés folyamatát dokumentálni kell, a dokumentálás történhet a Jogosultságigénylő lap kezelésével.

(2) A jogosultságkezelésre és a hozzáférés-ellenőrzésre vonatkozó részletes előírásokat, a jogosultságkezelés folyamatait a NKE Jogosultságkezelési és hozzáférési szabályzata tartalmazza, így különösen:

a) a jogosultságkezelés folyamatát munkatárs belépése, áthelyezése és kilépése esetén,
b) az informatikus munkatársak, privilegizált felhasználók jogosultságkezelési folyamatát munkatárs belépése, áthelyezése és kilépése esetén,
c) a külső munkatársak jogosultságkezelési folyamatát
d) munkatárs számára új jogosultság igénylésének és kezelésének folyamatát,
e) a felhasználói csoportok kezelésének folyamatát,
f) a kilépő munkatárs visszamaradó adatállománya kezelésének folyamatát (mentés, archiválás, törlés),
g) a jogosultság-felülvizsgálat folyamatát.

(3) Az egyes rendszerek esetében a speciális előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

(4) Az Egyetem kollégiumaiban és a rendezvények idejére biztosított hálózatokban nem kötelező az egyetemi felhasználói azonosítás. Ezekből a hálózati szegmensekből csak internet elérés biztosítható.

(5) Az Egyetem informatikai szolgáltatásai használatának jogosultsága az utolsó munkában töltött napig tart. Az illetékes rendszergazdák az Egyetemi elhagyási lap benyújtásakor, az azon megjelölt határidővel gondoskodnak a volt dolgozó jogosultságainak megszüntetéséről, törléséről. Egyedi méltánylást igénylő esetben – a szakterületért felelős magasabb vezető javaslatára – az INI igazgatója a hozzáférést meghosszabbíthatja.

(6) A munkavégzés során használt informatikai eszközökhöz való hozzáférés lejárta után 180 nappal a felhasználói fiók törlésre kerül.

XIII. FEJEZET
A HÁLÓZAT HASZNÁLATÁNAK BIZTONSÁGA
45. §

(1) Az Egyetem Hálózatát csak Magyarország hatályos jogszabályaiban és a vonatkozó szabályzatokban foglaltak szerint lehet használni. A Hálózatot – összhangban NIIFI program Felhasználói Szabályzatával – tilos használni az alábbi tevékenységekre, illetve ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

a) A mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, mások személyiségi jogainak megsértése (különösen: rágalmazás, stb.), tiltott haszonszerzésre irányuló tevékenység (különösen: piramisjáték, stb.), szerzői jogok megsértése (különösen: szoftver és médiatartalom nem jogszerű megszerzése, tárolása, terjesztése).

b) Másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységet bántó, zaklató tevékenység (különösen: pornográf, pedofil anyagok közzététele).

c) A hálózati erőforrások, szolgáltatások olyan célra való használata, amely az erőforrás/szolgáltatás eredeti céljától idegen (különösen: hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenet küldése).

d) Mások munkájának zavarása vagy akadályozása (különösen: kéretlen levelek, hirdetések).

e) A hálózati erőforrások magán célra való túlzott mértékű használata.

f) A hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (különösen: elektronikus levélbombák, hálózati játékok, kéretlen reklámok, online fájlmegosztás, digitális fizetőeszköz bányászat, stb.).

g) A Hálózat erőforrásaihoz, a Hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások – akár tesztelés céljából történő – illetéktelen szisztematikus próbálgatása (különösen: TCP/UDP port scan).

h) Hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (un. spoofing).

i) A Hálózat bármely szolgáltatásának szándékos, vagy hiányos ismeretekből, nem megfelelő körültekintéssel végzett beavatkozásokból fakadó zavarása, illetve részleges vagy teljes bénítása (leszámítva a rendeltetésszerű használat fenntartásához szükséges, a hálózati rendszergazdák, rendszermérnökök általi tudatos beavatkozásokat).

(2) A hálózati aktív eszközök feszültségmentesítését (kikapcsolását) áramszünet, természeti csapás (különösen: tűz, vízbetörés vagy más rendkívüli esemény), áramütés, vagy annak gyanúja, egyértelmű készülék meghibásodás (különösen: füst, látható zárlat vagy más látható műszaki hiba) kivételével csak az INI szakemberei végezhetik.

(3) Az Egyetemen az engedélyhez kötött rádiófrekvenciás tartományban sugárzó infokommunikációs eszközt kizárólag az INI igazgatója által engedélyezett frekvencián, az

engedélyezett időtartamra lehet használni és használata előtt legalább 30 nappal kell igényelni.

XIV. FEJEZET
INFORMATIKAI ESZKÖZÖK, ALAP PROGRAMCSOMAG BIZTONSÁGI ELŐÍRÁSAI
40. §

(1) Minden, a Hálózat használatára jogosultságot kapott felhasználó lehetőséget kap az alap-programcsomag használatára. A támogatott programok körét az INI az érvényes telepítési protokollban határozza meg.

(2) A folyamatos munkavégzésre kijelölt számítógépeken – az első Hálózatra kapcsolás előtt – az előzetes ellenőrzést, a használathoz előírt programok telepítését, valamint a feladatra történő felkészítést, a személyre-szabást az INI szakemberei az INI helyiségeiben hajtják végre.

(3) Az Egyetem alkalmazottainak a számítógépeket az INI az érvényes telepítési protokoll szerint előre telepített operációs rendszerrel, irodai programcsomaggal, vírusvédelmi szoftverrel és a hálózati szolgáltatások igénybevételére alkalmas programokkal, személyre szólóan felkészítve adja át.

(4) Ha a felhasználó számára kiadott számítógép a névre szóló felkészítés után másik felhasználóhoz kerül, akkor az új felhasználó feladata kezdeményezni az INI-nél, hogy a gép szoftverkonfigurációja, és a rá vonatkozó hálózati bejegyzések megfelelő módon, az INI szakemberei által módosításra kerüljenek.

(5) A számítógép hálózati beállításainak, rendszerelemeinek módosítására, az operációs rendszer és a gépre feltelepített szoftverek konfigurációjának megváltoztatására, szükség szerinti újratelepítésére vagy új programok telepítésére csak az INI szakemberei, illetve az általuk erre felhatalmazott és megfelelően felkészített személyek jogosultak.

(6) A Hálózatra csatlakoztatott informatikai eszközökön csak jogtiszta és az Egyetem által támogatott szoftverek körébe tartozó szoftverek telepíthetők és használhatók.

(7) Az eszközökön aktivizált automatikus programtevékenységeket (pl. vírusvédelmi szoftver működése) a felhasználó nem akadályozhatja. A felhasználói eszközök, különös tekintettel a mobil eszközökre (pl.: notebook) vonatkozó karbantartói feladatok ellátására, az eszközöket legalább 3 havonta az egyetemi hálózatra (és/vagy VPN kapcsolattal) kell csatlakoztatni, a karbantartás időtartamára. Amennyiben a karbantartó frissítések nem tudnak automatikusan megtörténni, felhasználó az INI kérésére 10 munkanapon belül az eszközt az INI ügyfélszolgálatára behozni köteles.

(8) A vezetői döntés alapján egyes munkatársak az Egyetem vagyonkezelésében lévő mobileszközöket, adattároló eszközöket (pendrive, külső meghajtó stb.) telefon előfizetést, adatkártyát is kaphatnak a napi munkavégzéshez.

XV. FEJEZET
EGYÉB BIZTONSÁGI SZABÁLYOK
Intranethasználat
46. §

Minden felhasználó jogosult a munkahelyi intranet használatára az Egyetem által biztosított és felügyelt informatikai eszközökkel, azonban a munkahelyi vezető dönthet a hozzáférés korlátozásáról.

Internethasználat biztonsági előírásai.
47. §

(1) Az Egyetem Hálózatán biztosított internetelérés a munkavégzést, az egyetemi célokat hivatott szolgálni, éppen ezért elsősorban az Egyetemen történő oktatással, kutatással, társadalmi élettel, munkaköri feladatokkal kapcsolatos feladatok felelősségteljes végzése támogatott.

(2) A Hálózatot használó munkaállomások alaphelyzetben (a speciális rendeltetésű számítógépek kivételével) rendelkeznek internet eléréssel. Az Egyetem fenntartja a jogot arra, hogy a vonatkozó törvények betartásával, és az azoktól kapott felhatalmazás alapján – különös tekintettel a Büntető Törvénykönyvben és az elektronikus hírközlésről szóló 2003. évi C. törvényben foglaltakra – az egyetemi Hálózat használata folyamán (a Hálózat biztonságos, és rendeltetés szerinti használatának, optimális leterheltségének, sebességének kialakítása, fenntartása érdekében) a felhasználók internetforgalmát, tartalmát figyelemmel kísérje és naplózza, a veszélyes internetes honlapok elérését letiltsa.

(3) A számítógépek és a Hálózat felhasználásánál a jelen Szabályzatban nem szabályozott kérdésekben a hatályos magyar jogszabályok irányadóak, különös tekintettel a Polgári Törvénykönyv és a Büntető Törvénykönyv, valamint a szerzői jogról szóló törvény vonatkozó rendelkezéseire. A hatályos jogszabályok rendelkezéseinek nem vagy nem kellő ismerete nem jelent mentesítést a megsértésük miatt kilátásba helyezett szankciók alkalmazása alól.

(4) A felhasználó az internetet elsősorban munkaköri feladatai ellátása, szakmai tájékozottsága növelése érdekében használhatja.

Levelezés biztonsági szabályai
48. §

(1) Az e-mail címek lehetnek személyhez, szervezethez vagy egyéb csoporthoz (pl. projekt) rendelve. Az Egyetem Hálózatán biztosított levelezés a munkavégzést, az egyetemi célokat hivatott szolgálni, éppen ezért elsősorban az Egyetemen történő oktatással, kutatással, társadalmi élettel, munkaköri feladatokkal kapcsolatos feladatok felelősségteljes végzése támogatott. Egyetemi e-mail cím kizárólag munkavégzéssel összefüggésben használható.

(2) Az előző pontban leírt célok elérése érdekében és szükség esetén – különösen biztonsági okokból – a Hálózat terheltségének csökkentése érdekében a külső levelező rendszerek elérése tiltásra kerülhet.

(3) Az INI az Egyetem állománya számára biztosítja az elektronikus levelezés lehetőségét. A szükséges e-mail címeket az INI-től az erre a célra rendszeresített igénylő lap kitöltésével lehet igényelni. Az igénylő lap kitöltésével és aláírásával a felhasználó elismeri jelen Szabályzat ismeretét és az abban tartalmazottak betartását.

(4) Az illetékes rendszergazda egységes algoritmussal – a benyújtott igénylőlap alapján, a felhasználónevéből, amelytől csak indokolt esetben, a felhasználóval történő egyeztetés után térhet el – határozza meg az e-mail címet, valamint gondoskodik a címek nyilvántartásáról, karbantartásáról. A hallgatói e-mail fiók neve a hallgató Neptun kódja. A rendelkezésre álló tárhely nagyságát, a küldhető, illetve fogadható levelek méretét a technikai lehetőségek függvényében az INI határozza meg.

(5) A jogviszony megszűnése után az egyetemi postafiók (levelezési cím) fenntartása, a használható postafiók méretének meghatározása a kilépő dolgozó szervezeti vezetőjének jóváhagyásával, és az INI igazgatóval történt egyeztetés után, egyedi elbírálás alapján történik.

(6) A jogviszony megszűnése után az egyetemi postafiók (levelezési cím) adattartalmát az INI lementi és azt 5 évig megőrzi. A megőrzési kötelezettség idejét követően INI jogosult a postaláda végleges törlésére. A törlési műveletet az INI dokumentálja.

(7) A jogviszony megszűnése után az egyetemi postafiókban munkavégzéssel összefüggésben kezelt személyes adatokat tartalmazó levelezésről készült másolatok kiadása – a GDPR 15. cikk (4) bekezdésére tekintettel – az Egyetem jogainak érvényesítése kapcsán korlátozható.

(8) A felhasználó által az (1) bekezdésében használt postafiókok esetében a postaládában szabályzatellenesen tárolt adatok az (6) bekezdésben rögzített időpontban és módon kerülnek törlésre.

(9) A megszűnés után az e-mail címet az INI 6 hónapig új belépő számára nem adja ki újra, ezen időtartamot követően az e-mail cím szabadon felhasználható.

49. §

(1) Az Egyetem működésével kapcsolatos levelezéshez, kiadványokban történő megjelentetéshez csak a hivatalos egyetemi e-mail címek használhatók.

(2) Az INI az egyes egyetemi szervezeteknek, illetve bizonyos, az Egyetem működéséhez kötődő speciális feladatok számára külön (kijelölt felelősökhöz kötött) szervezeti vagy (adott feladathoz létrehozott) tematikus email címet biztosít. Ezeknek az e-mail címeknek utalniuk kell a tulajdonos szervezetre, vagy az adott feladatra. Tilos ilyen célra a saját személyes e-mail címeket használni.

(3) A központi levelezés során a felhasználó levelezési forgalma (a kommunikációban résztvevő felhasználók felhasználói azonosítói, az igénybevett szolgáltatás típusa, a kommunikáció dátuma, kezdő és záró időpontja) naplózásra kerül (a levelek tartalma nem kerül rögzítésre).

(4) Az Egyetem címjegyzékeinek felhasználásával, szervezeti egységeknek szóló körlevél csak a saját szervezeti egysége vezetőjének engedélyével küldhető ki.

(5) Az Egyetem informatikai rendszerének működésével kapcsolatos technikai jellegű tájékoztatás egyetemi, kari szintű körlevelek küldésére az üzemeltetésért felelős rendszergazdák az üzemeltető egyetemi szervezet vezetőjének engedélyével jogosultak.

(6) Biztonsági és adatvédelmi okokból a beérkező levelek feltétel nélküli átirányítása csak az „uni-nke.hu" fődomain alatt üzemelő szerverekre engedélyezett, minden más levelező szerverre/domainre tiltott.

(7) Az Egyetem levelezőrendszere a nyílt interneten, webfelületen is elérhető. A levelező rendszer web felületen történő használata biztonsági okokból nagy körültekintést követel meg. Használata csak megbízható környezetben ajánlott.

(8) Amennyiben a felhasználó a postafiókjába 3 hónapon keresztül nem lép be, a postafiók – tartalmának változatlanul hagyása mellett – zárolásra kerül. A postafiók fogadja a leveleket, de a felhasználó nem tud belépni. További 3 hónap elteltével a fiók már leveleket sem fogad. Újabb 6 hónap (összesen 12 hónap) elteltével, a zárolás feloldására irányuló kérés hiányában, a felhasználói e-mail cím és a postafiók a tartalmával a (6) bekezdésben foglaltak szerint archiválásra kerül.

(9) Egyetemi e-mail címmel csak az egyetemi feladatokhoz szorosan kapcsolódó ismert, szakmai honlapokra engedélyezett regisztrálni és a belépési jelszónak az Egyetemen használt jelszótól különböző jelszót kell megadni. Minden más honlapon tilos az egyetemi, hivatalos e-mail cím használata.

(10) A személyhez rendelt e-mail címek képzésének módja: vezetéknév.keresztnév @uni-nke.hu. Azonos neveknél az egyediséget a vezetéknévk@uni-nke.hu módon képzett cím biztosítja.

(11) A felhasználó a postafiókját az interneten keresztül munkahelyén kívülről is el tudja érni.

WEB szerveren történő adattárolás, domain nevek használatának, tanúsítványok igénylésének szabályai
50. §

(1) Az Egyetem internetes megjelenítését biztosító web szervereit az INI üzemelteti, a megjelent tartalomért az alábbiak felelnek:

a) a kiemelt szervezeti egységek tartalmáért felelősek a *főszerkesztők*, aki az adott terület digitális megjelenésével kapcsolatos feladatokat látja el. A főszerkesztő feladatait tetszőleges számú (a tényleges tartalom feltöltést/törlés/módosítást elvégző) *szerkesztőre* delegálhatja, de a tartalmi megjelenésért, kizárólagos döntési jogkörrel és felelősséggel rendelkező funkciót a főszerkesztő egy személyében látja el;

b) az Egyetem egységes kommunikációjáért, sajtómegjelenéséért felelős szervezeti egység, a kommunikációs szakterület által kijelölt *felelős főszerkesztő*, akin keresztül a főszerkesztők munkáját, az egységes digitális megjelenést, az

Egyetem szabályzatainak való megfelelősség szempontjából (de nem tartalmilag!) felügyeli.

(2) A honlapon csak publikus, közérdekű és közérdekből nyilvános adatok jeleníthetők meg. Minősített adatok, információk megjelenítése tilos.

(3) Az egyes egyetemi szervezetekre vonatkozó információk tartalmáért, pontosságáért, naprakészségéért az adott szervezet vezetője a felelős.

(4) Az egyetemi honlapon történő adat/információ megjelenítésnél szigorúan be kell tartani a személyes és közérdekű, valamint a minősített adatok védelmére és biztonságára vonatkozó jogszabályokban és más közjogi szervezetszabályozó eszközökben (különösen a hatályos NKE Etikai kódexben és a biztonsági szabályzatokban) meghatározott előírásokat.

(5) Az egyes szervezeti egységek számára, a saját honlap rész kezeléséhez, az általuk megadott információk web felületen történő megjelenítéséhez – igény esetén – az INI szakemberei segítséget nyújtanak.

(6) Az Egyetem által használt, illetve az Egyetem életével kapcsolatos, internetes megjelenést szolgáló domain nevek igénylésére, kezelésére kizárólag az INI jogosult. Új domain név és SSL kapcsolatot igénylő szerver és felhasználói tanúsítványok, lejárt tanúsítványok helyett újak igénylése esetén az INI igazgatójához kell fordulni.

(7) Az Egyetem életével kapcsolatos események hivatalos internetes megjelentetésére elsődleges forrásként az ezeken a domain neveken belül üzemelő web felületek szolgálnak.

O365 felhőszolgáltatás biztonsági előírásai
51. §

(1) Az oktatók és a hallgatók közötti hatékony kommunikáció elősegítésére minden hallgató számára az O365 szolgáltatás keretén belül, felhőszolgáltatásként, az Egyetem biztosít saját e-mail címet (neptunkód@stud.uni-nke.hu), tárhelyet és hozzáférést az MS Office termékekhez.

(2) Az O365 felhő szolgáltatások elérésének központi oldala az **O365 PORTAL**, amely oldalon a hallgatók először az eddig is használt NEPTUN kód@stud.uni-nke.hu névvel és az eddig is használt születési dátumból generált standard jelszóval tudnak belépni, amit a belépést követően azonnal meg kell változtatni. Az egyetemi azonosítóval rendelkező felhasználók egyetemi e-mail címmel (felhasználó név@uni-nke.hu) mint felhasználónévvel és az egyetemi jelszavukkal tudnak belépni.

(3) Az O365 felhőszolgáltatásban működik a nagyszámú, egyidejű kép és hang továbbítást lehetővé tevő MS Teams alkalmazás, ami hallgatói hozzáféréssel vagy az egyetemi belépési felhasználó névvel, jelszóval érhető el. Távolléti oktatás esetén az MS Teams videokonferencia rendszere szolgáltatja az Egyetem virtuális oktatótermeit.

(4) Felhőszolgáltatás igénybevétele során az Egyetem – és jelen Szabályzat – biztonsági rendszabályainak betartása kötelező. A felhőszolgáltatás használata során **tilos** kritikus, a felhőszolgáltatás használatához nem szükséges személyes adat kategóriáiba tartozó adat,

valamint az Egyetem működése szempontjából bizalmas, továbbá minősített adat megosztása.

Digitális oktatási portál biztonsági előírásai
52. §

(1) Az oktatók a levelezéshez is használt azonosítójukkal és jelszavukkal, a hallgatók a Neptun kódjukkal és a születési dátumukból képzett jelszóval tudnak belépni a portálra.

(2) A Digitális oktatási portál portál igénybevétele során az Egyetem – és jelen Szabályzat – biztonsági rendszabályainak betartása kötelező.

Belső Képzési Portál biztonsági előírásai
53. §
https://belsokepzes.uni-nke.hu

(1) NKE azonosítóval elérhető képzési portál, ahol az egyetemi oktató anyagokon túl, a digitális oktatással kapcsolatos tájékoztatók, útmutatók, oktató videók folyamatosan elhelyezésre kerülnek.

(2) A Belső Képzési Portál igénybevétele során az Egyetem – és jelen Szabályzat – biztonsági rendszabályainak betartása kötelező.

Egységes HelpDesk portál
54. §
https://servicedesk.uni-nke.hu/

(1) Egységes HelpDesk (servicedesk) rendszer, amely csak belső hálózati eléréssel vagy VPN kapcsolattal hozzáférhető. Lehetőség szerint ezen a felületen kell minden informatikai bejelentést megtenni.

(2) Abban az esetben, ha sem belső, sem VPN elérés nem biztosított a servicedesk@uni-nke.hu címre is lehet bejelentéseket tenni, továbbá oktatás kapcsán vagy súlyos informatikai biztonsági esemény észlelése esetén kivételesen sürgős esetben rendelkezésre áll a 06303673462 ügyeleti telefon.

Saját eszközök használatának biztonsági előírásai
55. §

(1) Egyetemi célokra (munkavégzésre) a felhasználók saját, elsősorban mobil vagy esetleg más asztali számítástechnikai eszközeinek használatát a munkatárs munkahelyi vezetőjének javaslatára az INI igazgatója támogatásával – a megbízható hálózati működéshez és a védelemhez szükséges programok (különösen: vírusirtó program) INI által történt telepítése és nyilvántartásba vétele után – az Egyetem leltározási és leltárkészítési szabályzata szerint meghatározott bizonylat kitöltésével a gazdasági főigazgató engedélyezheti az alábbi feltételekkel:

a) A saját eszközön tárolt egyetemi (munkahelyi) adatok biztonságáért az eszköz tulajdonosa teljes körű felelősséggel tartozik.
b) A saját eszközön az operációs rendszer, biztonsági csomag, irodai rendszerek utolsó biztonságos frissítése használható, ezért javasolt aktivizálni ezek

automatikus frissítés funkcióját. (A biztonsági frissítéseket a programgyártók ingyenesen teszik elérhetővé.)

c) Saját eszközön bizalmas és minősített adatok tárolása tilos, azokon csak nyilvános adatok tárolása engedélyezett!

d) Az eszközt számítástechnikai hálózathoz, internethez csatlakoztatni csak biztonságos körülmények között szabad. A vezeték nélküli- WiFi-, bluetooth-kapcsolat csak biztonságos körülmények között használható, ezután kikapcsolásuk ajánlott (nyilvános helyeken – különösen szórakozóhelyek, üzletek, állomások területén elérhető hálózatok használata nem ajánlott).

e) A saját eszközön tárolt adatok (különösen: WiFi illetve bluetooth kapcsolaton keresztül) akár a tulajdonos, a használó tudtán kívül is lemásolhatók. Amennyiben a biztonsági esemény (különösen: az egyetemi adatok illetéktelen másolása, vagy a hitelessége, bizalmassága, sértetlensége egyéb módon sérül, stb.) az eszköz tulajdonosának gondatlanságából vagy neki felróható módon (különösen: program frissítések kikapcsolása, az eszköz gondatlan tárolása, szállítása, stb.) következik be, az így okozott károkért teljes körű felelősséggel tartozik.

f) A saját eszközön történő egyetemi feladatokkal kapcsolatos munkavégzéshez szükséges adatokat külön könyvtárban (könyvtárrendszerben) kell tárolni, amely kialakításához – kérés, szükség esetén – az INI szakemberei segítséget nyújtanak, illetve az eszközt érintő biztonsági esemény esetén az INI szakemberei részére hozzáférést kell biztosítani. Egyúttal ki kell jelölni az egyetemi Hálózatra történő mentések helyét.

g) A munkahelyi célokra létrehozott könyvtárak egyetemi Hálózatra történő rendszeres mentésére fokozott figyelmet kell fordítani. A Hálózatra történő mentés a felhasználó kötelessége.

h) A jogviszony és a hozzáférési engedély megszüntetése után az egyetemi munkavégzéssel kapcsolatos adatokat, és az egyetemi licencek alapján telepített programokat az eszközről visszaállíthatatlanul törölni kell, amit végezhet az INI illetékes szakembere, vagy az eszköz tulajdonosa, használója. A visszaállíthatatlan törlést végző személy írásos nyilatkozatot tesz a végrehajtásról.

(2) Időszakos rendezvényeken (különösen: konferenciákon, gyakorlatokon, stb.) külön erre a célra, az adott időtartamra létrehozott zónákban külön engedély nélkül lehet a saját mobil eszközöket használni.

(3) Különös figyelemmel kell lenni a munkatársak saját eszközeinek biztonságos használatára, amellyel nem sérthetők sem a személyes, sem az egyetemi érdekek. Vitás esetekben az egyetemi érdekek elsőbbséget élveznek és a saját eszközök használatát – indokolt esetben – az egyetemi Hálózat biztonságának veszélyeztetése esetén – akár figyelmeztetés nélkül – azonnal, más esetekben 24 órával korábban történt figyelmeztetés után, fel lehet függeszteni, meg lehet tiltani, akadályozni, vagy egyes hálózati szolgáltatások elérhetőségét korlátozni.

Közösségi hálózatok biztonságának szabályai
56. §

(1) Az Egyetem használni kívánja az internetes közösségi oldalakat is tevékenységének széleskörű megismertetésére, társadalmi elfogadottságának növelésére, oktatói tevékenységének a továbbtanulás előtt álló középiskolások közötti népszerűsítésére.

(2) Az Egyetem rendelkezik több internetes közösségi honlapon saját fórummal, amelyek az Egyetem életével kapcsolatos események hivatalos internetes megjelentetésére, véleményformálásra szolgálnak.

(3) Internetes közösségi és más nyilvános oldalakon történő megnyilatkozások esetében is figyelemmel kell lenni a személyes és közérdekű adatok védelmére és biztonságára vonatkozó jogszabályokban és más szervezetszabályozó eszközökben (különösen a hatályos NKE Etikai kódexben és a biztonsági szabályzatokban) meghatározottakra, ugyanis ezek a megnyilatkozások nem csak a kinyilvánítójuk, hanem az Egyetem jó hírnevére is befolyással lehetnek és akár jogi következményekkel is járhatnak.

(4) Az Egyetem vezetése elvárja, hogy az Egyetem alkalmazottai és hallgatói megnyilatkozásaik folyamán személyes identitásukat nem elfedve képviseljék véleményüket, amelyért felelősséggel tartoznak. Az Egyetem tevékenységében esetlegesen meglévő hiányosságokat, a belső vitákat nem a nyilvános, hanem a belső fórumokon kell megvitatni. Tilos az Egyetemmel, a vezetésével, munkatársaival, hallgatóival kapcsolatosan az Egyetem alkalmazottaihoz, hallgatóihoz méltatlan (különösen valótlan, fenyegető, obszcén, vulgáris, stb.) vélemények nyilvános közlése. Az interneten megjelenő véleménynyilvánítások kapcsán minden megnyilatkozónak szem előtt kell tartania, hogy ami az interneten egyszer megjelenik, az a későbbiekben már nem, vagy csak rendkívüli erőfeszítésekkel törölhető.

Szoftverjogtisztaság, szoftverek telepítése, frissítése
57. §

(1) A szoftverek jogtisztaságának kérdése kiterjed a beszerzés, az üzemeltetés, a licencelés kérdéseire és megfelel a jogi, a pénzügyi és technikai követelményeknek.

(2) A számítógépekre csak jogtiszta szoftverek telepíthetők.

(3) A telepített szoftverek (és hardverek) nyilvántartását a Novell Zenworks Inventory teszi lehetővé.

(4) Az Egyetem belső és tantermi zónáiban üzemelő felhasználói munkaállomásokon telepített operációs rendszerek, irodai szoftverek frissítése – jelenleg – az interneten keresztül automatikusan történik. A frissítési folyamat felhasználói beavatkozást nem igényel.

(5) Az Egyetem által üzemeltetett infokommunikációs eszközökre programok telepítése történhet:
- *a)* az üzemeltetési szakterület által központilag,
- *b)* az üzemeltetési szakterület erre felhatalmazott munkatársai által manuálisan.

(6) A felhasználó az eszközökre telepített szoftverek beállításait csak a jogosultsága által engedélyezett mértékben változtathatja meg. A beállított korlátozások bármilyen eszközzel történő megkerülése tilos.

(7) Az engedély nélkül, vagy a korlátozás megkerülésével a felhasználó által esetlegesen telepített szoftvereket az INI a felhasználó tájékoztatása mellett törölheti.

Elektronikus tárhelyek igénybevétele, dokumentum-megosztás, munkahelyi adatok mentése
58. §

(1) A felhasználói irodai munkakörnyezethez az Egyetem központi elektronikus tárhelyeket biztosít (fájlszerver területek) az alábbiak szerint:

a) a felhasználó személyes központi tárhelyéhez csak a felhasználó kap – teljes körű (olvasási, írási, módosítási, törlési jogot tartalmazó) – hozzáférést,

b) a szervezeti egység privát központi tárhelyéhez a szervezeti egység munkatársai kapnak – teljes körű – hozzáférést,

c) a szervezeti egység publikus központi tárhelyéhez a szervezeti egység vezetője engedélyez a szervezeti egységen kívüli munkatársaknak – teljes körű vagy egyes jogokra korlátozott – hozzáférést.

(2) A Hálózatba kapcsolt munkaállomások esetében a felhasználó felelőssége, hogy a munkahelyi feladataival kapcsolatos adatokat, dokumentumokat az Egyetem által biztosított központi tárhelyre mentse.

(3) A hálózatba kapcsolt munkaállomás lokális tárhelyére (C vagy D meghajtó) menteni csak indokolt esetben, ideiglenesen megengedett (pl. a Hálózat kiesése esetén vagy a használt alkalmazás követelménye miatt), és az így mentett adatokat a lehető leghamarabb át kell másolni a központi tárhelyre. A hálózatba kapcsolt munkaállomás lokális tárhelyéről mentés nem készül.

(4) A felhasználó felelőssége, hogy a Hálózatba nem kapcsolt informatikai eszközökön tárolt, a munkahelyi feladataival kapcsolatos adatokról, dokumentumokról biztonsági mentéseket készítsen.

(5) A lokális tárhelyre mentett vagy a Hálózatba nem kapcsolt informatikai eszközökön tárolt adatvesztés esetén az ezzel kapcsolatos minden felelősség a felhasználót terheli.

(6) A felhasználó rendelkezésére bocsátott eszközökön kizárólag a munkahelyi feladatok ellátásához szükséges adatok, dokumentumok tárolandók.

(7) Központi (hálózati) tárterületen tilos tárolni bármilyen, a munkavégzéshez nem kapcsolódó adatot, dokumentumot. A magáncélú adatokat, dokumentumokat a felhasználónak kell saját tulajdonú adathordozóra mentenie.

(8) Az Egyetem fenntartja magának a jogot, hogy azokat az adatokat, dokumentumokat, amelyek valamilyen jellemzőjük (fájltípus, név) alapján feltehetően nem kapcsolódnak a felhasználó munkavégzéséhez, előzetes figyelmeztetést követően törölje.

(9) A nem munkahelyi célra készített vagy tárolt adatok károsodásáért, megsemmisüléséért az Egyetem semmilyen felelősséget nem vállal.

59. §

(1) A központi tárhelyen tárolt adatokról az Egyetem mentést készít, ami lehetővé teszi az adatok visszaállítását.

(2) Az adatok, dokumentumok visszaállítása az INI-től kérhető, a dokumentum vagy könyvtár nevének és pontos elérésének megadásával.

(3) Azon felhasználók, akiknek jogviszonya megszűnik, a jogviszony megszűnésétől számított 6 hónapot követően, a személyes központi tárhelyen tárolt adatait az INI törli.

(4) A több felhasználó által közösen használt adatok biztonságos, illetéktelen hozzáféréstől védett elhelyezésére az INI a szervereken szükség szerint tárhelyet biztosít. A tárterülethez történő hozzáférés beállítása az adatokért felelős személy írásos igénye alapján történik.

(5) A fájlok elérési útvonalának a teljes hossza maximum 256 karakter lehet, amelybe a könyvtárstruktúrát alkotó könyvtárak nevei, a fájlnév és a kiterjesztés (pl.:.docx) is beleértendő (pl.: S:\könyvtár\alkönyvtárA\alkönyvtárAB\alkönyvtárABC\irat.doc). Az archiválás, és a rendszerek közti hordozhatóság miatt javasolt még a kisbetűk használata és a szóközök kerülése a mappa-, fájlnevekben. A megnevezésekben kerülni kell az ékezetes magyar magánhangzók – legfőképpen az í, Í, ő, Ő, ú, Ú, ű, Ű – használatát, mivel egyes rendszerek nem tudják helyesen kezelni ezeket a karaktereket.

(6) A könyvtárakat egymásba ágyazni központi (hálózati) tárhelyen (S és T meghajtó) maximálisan 3 mélységig megengedett.

(7) A felhasználók a tanulmányi, oktatói, munkahelyi tevékenységükkel kapcsolatosan keletkezett adatokat a hálózati szervereken a számukra kijelölt könyvtárakban helyezhetik el. Ez a tárterület csak e tevékenységekkel kapcsolatos adatok tárolására használható. A könyvtárak elnevezéseinek, felhasználásuk céljainak, hozzáférési jogosultsági rendszerének beállítása az adatfelelős és a rendszergazda közös feladata. A könyvtárak elnevezésének egyértelműen utalnia kell a benne elhelyezett tartalomra. A területek adattartalmáért a jogosult felhasználók és a terület adatgazdája felel.

(8) A Hálózat tárterületével történő gazdálkodás az INI feladata és felelőssége. Az Egyetem vagyonkezelésében lévő eszközök (vagyontárgyak csak az Egyetem vagyonkezelésében levő adatok tárolására használhatók. A központi tárhelyen tárolt nem közérdekű vagy az aktualitásukat veszített közérdekű tartalmakat (különösen: videók, fényképek, és más hasonló jellegű adatállományok), amennyiben a munkavégzést akadályozzák akár azonnal, ellenkező esetben a tulajdonos értesítését követő 24 óra elteltével az INI hálózati rendszergazdája jogosult törölni.

XVI. FEJEZET
MOBIL ADATHORDOZÓK KEZELÉSE
60. §

(1) Az Egyetem vagyonkezelésében levő mobil adathordozók kizárólag munkavégzéssel összefüggő célokra használhatók. Alkalmazásuk abban az esetben engedélyezett, ha a

gazda eszköz (számítógép, tablet stb.) menedzselt eszköz és képes a csatlakoztatott mobil adathordozón kártékonykód-ellenőrzést végezni.

(2) A mobil adathordozókat a rajtuk tárolt vagy tárolandó adatok védelmi előírásainak megfelelően kell kezelni.

(3) A mobil adathordozók azonosítását nyilvántartási szám feltüntetésével (címkézés), mozgásuk nyomon követhetőségét az átadás-átvétel, továbbítás, selejtezés, megsemmisítés dokumentálásával biztosítani kell. Amennyiben a címkézés nem kivitelezhető, egyedi módon szükséges gondoskodni az azonosításról (pl. kísérő lap a gyárilag beépített adathordozók esetében).

Adatmentesítés
61. §

(1) A mobil adathordozók esetében alkalmazandó adatmentesítési eljárás az üzemeltetési alapeljárásban történő adattörlés.

(2) Az üzemeltetési alapeljárásban történő adattörlést (formattálás, image készítése) az adathordozó újbóli használatra alkalmassá tétele érdekében az üzemeltetési szakterület munkatársa napi tevékenysége során hajtja végre a vonatkozó folyamatleírásban foglalt szabályok szerint.

(3) Amennyiben az adathordozón tárolt adatok érzékenysége indokolja, az érintett felhasználó külön eljárásban kéri és, ha a rendelkezésre álló törlőeszköz ezt lehetővé teszi, a biztonságos adattörlést a felhasználó objektumában és jelenlétében is végre lehet hajtani.

XVII. FEJEZET
AZ INFORMATIKAI FEJLESZTÉSEK
Általános rendelkezések
62. §

(1) A fejlesztés során folyamatosan biztosítani kell, hogy az INI a fejleszteni tervezett rendszer, infokommunikációs eszköz, informatikai szolgáltatás informatikai biztonsági aspektusait ellenőrizhesse.

(2) A fejlesztés és a változáskezelés folyamataiba az információvédelmi ellenőrzést be kell építeni.

(3) Fejlesztési tevékenység csak az INI ilyen rendeltetésű rendszereiben végezhető. Ezen előírás teljesítése alól az INI igazgatója felmentést adhat.

(4) A fejlesztésekhez és a tesztelésekhez éles rendszerből kinyert személyes adatok kizárólag anonimizált módon használhatók fel.

(5) Új rendszer, rendszerelem, infokommunikációs eszköz, szoftver vagy szoftververzió rendszerbe állítását az üzemeltetési szakterület érintett szervezeti egységének vezetője engedélyezi.

A fejlesztési folyamat dokumentálása
63. §

(1) A fejlesztő köteles a fejlesztési folyamatot úgy dokumentálni, hogy a fejlesztési folyamat során elvégzett tevékenységek és a készített dokumentumok egymásnak megfeleltethetők legyenek. A fejlesztés során készülő dokumentumokat verziókezelten, rendszerenként elkülönítve, elektronikusan, visszakereshető formában kell tárolni.

(2) A fejlesztések tervezése során az informatikai szakmai követelmények meghatározásáról és megfelelő dokumentálásáról a fejlesztő gondoskodik.

(3) Az informatikai szakmai követelmények meghatározásának része a biztonsági követelmények meghatározása és teljesítésük módjának rögzítése, így különösen

a) a rendszerbiztonsági terv,
b) az információbiztonsági architektúra leírás elkészítése.

Fejlesztői változáskövetés
64. §

A fejlesztői változáskövetés szabályozása és megvalósítása során biztosítani kell az alábbiakat:

a) a változtatásokat minden esetben a fejlesztésre irányadó szabályok szerint dokumentálni kell,
b) a változtatások lehetséges biztonsági hatásait a végrehajtás előtt értékelni kell,
c) csak a jóváhagyott változtatások hajthatók végre,
d) a változtatások okáról és tartalmáról az üzemeltetésért felelős szervezeti egységet az általa meghatározott módon tájékoztatni kell,
e) biztonsági frissítést nyújtsanak legalább 5 évig.

Tesztelés
65. §

(1) A fejlesztési, tesztelési és működési környezetet el kell választani, hogy csökkenteni lehessen a jogosulatlan hozzáférés vagy változtatás kockázatát a működési környezetben. Ezen előírás teljesítése alól csak az INI igazgatója adhat felmentést.

(2) A rendszer, rendszerelem, infokommunikációs eszköz megfelelőségének értékeléséhez szükséges tesztelési folyamatok megtervezéséről és végrehajtásáról az INI gondoskodik.

(3) A tesztelési folyamatokra vonatkozó részletes előírásokat az Egyetem Tesztelési folyamat szabályzata tartalmazza.

(4) A tesztelésre vonatkozó előírások teljesítéséért a fejlesztő – az üzemeltető bevonásával – a felelős.

(5) Tesztelési tevékenység csak az Egyetem ilyen rendeltetésű rendszereiben végezhető. Ezen előírás teljesítése alól a fejlesztést, beszerzést kezdeményező INI igazgató felmentést adhat.

Fejlesztők általi oktatás
66. §

A fejlesztett rendszer fejlesztője köteles a szervezet kijelölt informatikus munkakört betöltő munkatársai számára oktatást biztosítani, amelyen a rendszer működésével és használatával összefüggő ismeretek elsajátíthatók.

XVIII. FEJEZET
INFORMATIKAI ÜZEMELTETÉS

67. §

(1) A rendszerek rendeltetésszerű működéséért, rendelkezésre állásáért az üzemeltető szervezeti egység vezetője felel.

(2) Az egyes rendszerekre vonatkozó előírásokat a rendszerüzemeltetési szabályzat/ kézikönyv tartalmazza.

Karbantartás biztonsági szabályai
68. §

(1) A rendszerek, infokommunikációs eszközök adattárolást megvalósító elemei és az adathordozók az Egyetemmel polgári jogi jogviszonyban álló személyek általi karbantartásra, javításra, cserére csak a tárolt adatállomány biztonságos törlését követően adhatók át. A törlés megvalósításért személyes használatú eszköz esetében a felhasználó, központilag bonyolított karbantartás, javítás, csere esetén az eljáró szervezeti egység vezetője felel.

(2) Az NKE, mint megrendelő által kötött, támogatói (ún. support) tevékenységre vonatkozó szerződések esetében adatállományt tartalmazó adattárolást megvalósító rendszerelemek és adathordozók csak a support tevékenység végzésének elősegítése (pl. hibakeresés) céljából adhatók ki. Amennyiben lehetséges, az adatállományok megismerhetőségét ezekben az esetekben is korlátozni kell (pl. rendszer felépítésére vonatkozó adatok maszkolása, személyes adatok anonimizálása stb.). Az adatállomány kiadhatóságáról az üzemeltetési szakterület vezetője dönt.

Hibakezelés
69. §

Az egyes rendszerekre vonatkozó előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

Változáskezelés
70. §

Az egyes rendszerekre vonatkozó előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

Konfigurációkezelés
71. §

Az egyes rendszerekre vonatkozó előírásokat a rendszerüzemeltetési szabályzat/ kézikönyv tartalmazza.

Naplózás és naplóelemzés
72. §

(1) A rendszer használatával összefüggő eseményeket a rendszerben naplózni kell. Ez a rendelkezés vonatkozik az üzemeltetési, rendszerfelügyeleti, rendszerbiztonsági feladatok ellátására is. Naplózási eljárásrendet kell létrehozni, amiben az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

(2) A naplózás kialakításakor a rendelkezésre álló erőforrások függvényében törekedni kell a naplózási célt teljesítő, hatékony és az elérhető legfejlettebb technológián alapuló megoldások alkalmazására.

(3) A rendszer fejlesztése, továbbfejlesztése és üzemeltetése során a rendszer megfelelőségének (bizalmasság, sértetlenség, rendelkezésre állás) ellenőrzését szolgáló naplóállományok tartalmát, rögzítésének, tárolásának és ellenőrzésének módját az üzemeltetésért felelős szervezeti egység határozza meg a naplózási eljárásrendben.

(4) Az egyes rendszerek működésével összefüggő naplóállományokat együttesen kell kezelni (gyűjteni, tárolni, archiválni, megsemmisíteni).

XIX. FEJEZET
KÁRTÉKONY KÓDOK ELLENI VÉDELEM
Általános rendelkezések
73. §

(1) A kártékony kódok elleni védelmi eljárásokat, a vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy azok az elektronikus információs rendszert annak belépési és kilépési pontjain védjék a kártékony kódok ellen, felderítsék és megsemmisítsék azokat, valamint:

a) a folyamatos felügyelet ellátását lehetővé tegyék,
b) támogassák a valós riasztások kiszűrését,
c) alkalmasak legyenek a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,
d) tegyék lehetővé a kártékony kódok elleni védelem általános helyzetének értékelését,
e) biztosítsák az új fenyegetések időben történő felismerését, frissítsék a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg,
f) tegyék lehetővé a riasztások és a védelmi rendszer állapotában bekövetkező változások naplóelemző rendszerbe történő továbbítását.

(2) A kártékony kódok elleni védelemmel kapcsolatos üzemeltetési feladatokat az INI látja el.

A kártékony kódok elleni védelmi eszközök és eljárások alkalmazása
74. §

(1) A számítógép számítógépes vírussal vagy más rosszindulatú programmal, történő fertőződése súlyos biztonsági kockázat. Az Egyetem Hálózatában az INI által központilag biztosított, felügyelt többszintű vírusvédelmi rendszer működik. Ha ennek ellenére valamelyik számítógép, felhasználói munkaállomás vírussal fertőződik, az INI – a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében – kizárhatja azt a hálózati forgalomból. A felhasználó ilyen esetben köteles a mielőbbi vírusmentesítés érdekében együttműködni az INI munkatársaival.

(2) Több munkaállomás számítógépes vírusfertőzése esetén a vírusmentesítés és az ellenőrzések idejére, a fertőzés terjedésének megakadályozása érdekében az INI jogosult az adott hálózati szegmens izolálására vagy kizárására.

(3) A felhasználóknak be kell tartaniuk a vírusvédelemre vonatkozó elemi szabályokat és az ide vonatkozó egyéb rendelkezéseket.

(4) A vírusvédelmi rendszer frissítése központilag, felhasználói beavatkozás nélkül történik, amelyet a vírusvédelmi rendszer szervergépe hajt végre az Egyetem belső és tantermi zónáiban üzemelő felhasználói munkaállomásokon. A szerver elérhetetlensége esetén a munkaállomások vírusvédelmi rendszerének frissítése az interneten keresztül történhet.

(5) Ha a vírusvédelmi rendszer nem működik a munkaállomáson (a Windows tálcán nem látható annak ikonja vagy hibát jelez), a felhasználó köteles azt azonnal az INI-nek jelenteni. A vírusvédelmi rendszer helyreállításáig a felhasználó mobil adathordozót nem kezelhet a munkaállomásán, illetve mobil munkaállomás esetén internetre, Hálózatra nem csatlakozhat.

(6) Ha a felhasználó rosszindulatú szoftver, kártékony kód jelenlétére gyanakszik, az INI-t kell értesítenie és a gyanús eszköz vagy rendszer használatát lehetőleg fel kell függesztenie.

XX. FEJEZET
TITKOSÍTÁS
75. §

(1) Kizárólag közérdekű és közérdekből nyilvános adatok esetében a titkosítás alkalmazása nem kötelező.

(2) Nem a fenti adatkörbe tartozó adatok, így különösen törvény által védett adatok, titkok esetében a titkosításról, illetve – amennyiben a titkosítás alkalmazása lehetetlen vagy alkalmazása aránytalan nehézséggel vagy költséggel járna – kockázatcsökkentő intézkedésekről kell gondoskodni.

(3) A titkosítás végrehajtásáért a rendszert üzemeltető, adatot tartalmazó adathordozó, eszköz esetében az adatgazda, illetve az adathordozót használó vagy szállító személy felel.

(4) Az egyes rendszerek esetében a speciális előírásokat a rendszerüzemeltetési szabályzat/kézikönyv tartalmazza.

XXI. FEJEZET
ZÁRÓ RENDELKEZÉSEK
76. §

(1) A jelen Szabályzatot a Szenátus 102/2020. (IX. 23.) számú határozatával fogadta el.

(2) A jelen Szabályzat 2020. október 1-jén lép hatályba.

(3) A jelen Szabályzat hatálybalépésével egyidejűleg hatályát veszti Szenátus 131/2017. (XII. 06.) sz. határozatával elfogadott elfogadott Informatikai Biztonsági Szabályzat.