**A Pécsi Tudományegyetem**
**Informatikai Biztonsági Szabályzata**

**Pécs**
*Hatályos 2025. január 1. napjától*

Tartalom

## Preambulum

A Pécsi Tudományegyetem (továbbiakban: Egyetem) az oktatási, egészségügyi, kutatási, fejlesztési, adminisztratív feladatok támogatása, valamint az információ szabad áramlása, az adatok-, az információk- és a tudáshasznosítás informatikai eszközökkel történő védelmének biztosítása érdekében, valamint a nemzeti felsőoktatásról szóló 2011. évi CCIV. (továbbiakban: Nftv.) törvényben foglaltakat figyelembe véve; továbbá létfontosságú rendszerelem üzemeltetőként az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban Ibtv.) előírtak megvalósítása és a 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 szerint a kijelölt rendszerelemek biztonsági osztályba, és az Egyetem, valamint egyes szervezeti egységek biztonsági szintbe sorolása érdekében az Egyetem Informatikai Biztonsági Szabályzatát (továbbiakban: Szabályzat) az alábbiak szerint határozza meg:

## 1. fejezet Általános rész

### A szabályzat célja

**1. §** (1) A Szabályzat alapvető célja, hogy az Egyetem működése során előírja az Egyetemhez kapcsolódó bármely tevékenységek során betartandó információbiztonsági szabályokat, irányelveket és felelősségi köröket.

(2) A Szabályzat célja a PTE működéséhez elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.

(3) A Szabályzat a fentiek megvalósítása érdekében keretjelleggel – a hatályos jogszabályokkal és az Egyetem belső szabályzataival, így különösen a Pécsi Tudományegyetem Informatikai Szabályzatával összhangban – meghatározza a rendszerekre és a rendszerekkel kapcsolatos tevékenységekre vonatkozó adminisztratív, fizikai és logikai követelmények elérésével és fenntartásával összefüggő garanciális folyamatokat, feladatokat és felelősségeket. A vonatkozó részletszabályokat jelen Szabályzat felhatalmazása alapján kancellári utasításban szükséges meghatározni.

(4) Az Egyetem nagy mennyiségű és heterogén adatot (személyes, gazdasági, gazdálkodási, kutatási, oktatási, egészségügyi) kezel, amiknek az eszmei értéke felbecsülhetetlen, értékben nem kifejezhető. Így ezek védelme a bizalmasság, sértetlenség és rendelkezésre állás kritériumok biztosításához kiemelt stratégiai fontosságú, összetett és csak közös akarattal megvalósítható feladat.

(5) A Szabályzat aktualizálása az Információbiztonsági Felelős (továbbiakban IBF) felelőssége.

### A szabályzat hatálya

**2. §** (1)A Szabályzat személyi hatálya kiterjed:

a) PTE SZMSZ 77-78. §-okban meghatározott karokon, önálló szervezeteknél, valamint az Egyetem által fenntartott köznevelési és szakképző intézményekben foglalkoztatott, egészségügyi szolgálati jogviszonyban vagy munkaviszonyban álló, valamint az Egyetemmel, vagy szervezeti egységeivel munkavégzésre irányuló egyéb jogviszonyban (továbbiakban: foglalkoztatott) álló személyekre;
b) az Egyetemmel hallgatói, vagy egyéb képzési jogviszonyban álló személyekre (továbbiakban: hallgató);
c) az Egyetemmel szerződéses vagy egyéb jogviszonyban álló természetes és jogi személyekre, amennyiben azok hozzáférést kapnak az Egyetem informatikai erőforrásaihoz, rendszereihez;
d) az Egyetemmel szerződéses jogviszonyban nem álló bármely természetes és jogi személyre, amennyiben az Egyetem által nyújtott informatikai szolgáltatásokat igénybe veszik (továbbiakban együttesen: felhasználókra).

(2) A szabályzat területi hatálya kiterjed:
a) az Egyetem teljes területére;
b) az Egyetem tulajdonában vagy használatában lévő informatikai eszközöknek az Egyetem területén kívül történő igénybevétele esetén az igénybevétel helyére (pl. hordozható eszköz otthoni munkavégzéshez);
c) az Egyetem területén kívül, idegen eszközön történő igénybevétel esetén az igénybevétel helyére (pl. saját tulajdonú eszközről távoli eléréssel).

(3) A Szabályzat tárgyi hatálya kiterjed
a) az Egyetem teljes hálózati infrastruktúrájára;
b) Egyetem minden információkezeléssel és feldolgozással kapcsolatos folyamatában résztvevő informatikai eszközre, nyilvántartást strukturáltan megvalósító rendszerre, mely az Egyetem területén található, illetve ezen eszközök elhelyezésére szolgáló létesítményekre;
c) az Egyetem tulajdonában vagy használatában lévő informatikai eszközökre és az informatikai eszközök által kezelt, tárolt, továbbított adatokra, információkra, a szoftverek teljes körére;
d) az Egyetem informatikai hálózatára csatlakozó, de nem az Egyetem tulajdonában lévő eszközökre, függetlenül azok földrajzi elhelyezkedésére.

Általános rendelkezések

**3. §** (1)A Szabályzatban alkalmazott meghatározásokat az 1. számú melléklet (Fogalomtár) tartalmazza.

(2) A vonatkozó jogszabályok, további belső szabályzatok a 2. számú mellékletben (Kapcsolódó jogszabályok, szabályozások listája) találhatóak.

(3) A Szabályzat, szabályzathoz tartozó eljárásrendek felülvizsgálatát el kell végezni az alábbi esetekben:
a) két éves rendszerességgel, valamint;
b) szervezeti, infrastrukturális, informatikai erőforrásokban bekövetkező változások, tevékenységi körben, folyamatokban történő jelentős változások, jelentős személyi változások, magasabb szintű belső szabályzatokban történt módosítások, jogszabályi változások esetén eseti jelleggel, valamint;
c) amennyiben egy súlyos incidenst követően az Informatikai Bizottság erre javaslatot tesz;
d) bármikor, a Kancellár vagy IBF, vagy az informatikai igazgató kezdeményezésére.

(4) A felülvizsgálat során az alábbi szempontokat kell figyelembe venni:
a) kockázatok azonosítása és kezelése: a kockázatkezelési eljárások hatékonysága, valamint az újonnan azonosított kockázatok kezelése;
b) biztonsági incidensek: a biztonsági incidensek számának és súlyosságának alakulása, valamint a válaszintézkedések hatékonysága;
c) képzések hatékonysága: a munkavállalók információbiztonsági képzéseinek eredményessége és hatása a tudatosságra;
d) szabályzatok és eljárások: az információbiztonsági szabályzatok és eljárások aktualitása és megfelelősége.

(5) A felülvizsgálat eredményeit dokumentálni kell egy felülvizsgálati jelentés formájában, amely tartalmazza:
a) a felülvizsgálat dátumát és a résztvevőket;
b) a kiértékelési szempontok alapján tett megállapításokat;
c) ajánlásokat a szükséges módosításokra és fejlesztésekre.

(6) A felülvizsgálat során tett ajánlások végrehajtásáért az IBF felel. A végrehajtott intézkedéseket nyomon kell követni, és a haladást rendszeresen jelenteni kell az Egyetem vezetősége felé.

## 2. fejezet Az információbiztonsági rendszer

Alapelvek

**4. §** (1) 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;
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

(2) Kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni az Egyetemen.

Vezetői elkötelezettség

**5. §** (1) Minden szervezeti egység vezetője aktívan hozzájárul az információbiztonság kultúrájának kialakításához és fenntartásához.

(2) A vezetők elkötelezettségüket személyes példamutatással, személyes felelősségvállalással, a szabályok teljeskörű betartásával és betartatásával demonstrálják.

(3) Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása az Egyetem vezetőinek a felelőssége a Pécsi Tudományegyetem Szervezeti és Működési Szabályzatában (továbbiakban: SZMSZ) meghatározottak szerint.

(4) A vezetők megkövetelik és elősegítik az információbiztonsági követelmények megismertetését és betartatását a szervezeti egységükhöz tartozó munkavállalókkal.

Az információbiztonsági rendszer kialakítása és működtetése

**6. §** (1) A jelen Szabályzat egységes rendszerbe foglalja az Egyetem információbiztonsági feladatait, így felkészítve az Egyetemet az információbiztonságot fenyegető veszélyekkel szemben történő szervezett védekezésre.

(2) Az információbiztonsági rendszer célja, hogy megfelelő védelmet nyújtson az Egyetem informatikai rendszereiben és hálózataiban kezelt adatok számára, biztosítva azok bizalmasságát, sértetlenségét és rendelkezésre állását.

(3) Az Egyetem szervezeti egységei által használt informatikai infrastruktúra védelméért a szervezeti adatgazdák, az Informatikai Igazgatóság és az IBF közösen felelnek. Az információbiztonság teljes körű, és folytonos biztosítása érdekében a feladatokat és felelősségeket az alábbiak szerint határozhatóak meg:

a) Kockázatelemzés és -kezelés:
   - felelős szakterület: IBF
   - feladat: évente, illetve szükség esetén kockázatelemzést végez a 2§ (4.) alapján, melynek célja a biztonsági kockázatok azonosítása és kezelése. Biztosítja, hogy a fenyegetések és sebezhetőségek feltérképezése után a megfelelő intézkedéseket megfogalmazzák, és megvalósítsák;
b) Biztonsági politikák és eljárások kialakítása:
   - felelős szakterület: IBF, együttműködve az Informatikai Igazgatósággal
   - feladat: az IBF kialakítja és évente felülvizsgálja a biztonsági politikákat és eljárásokat, amelyek az információbiztonsági követelményeket tartalmazzák. Az Informatikai Igazgatóság támogatja a folyamatot az informatikai infrastruktúrával kapcsolatos szakmai információval és technikai megoldásokkal;

c) Fizikai és logikai biztonság:
   - felelős szakterület: Informatikai Igazgatóság, együttműködve az IBF-el.
   - feladat: az Informatikai Igazgatóság felelős az informatikai rendszerek és hálózatok fizikai és logikai biztonságáért, ideértve a hozzáférés-ellenőrzést, tűzfalakat, vírusvédelmet és titkosítást. Az IBF biztosítja, hogy a biztonsági intézkedések megfeleljenek a szervezeti előírásoknak és jogszabályi követelményeknek;
d) Oktatás és tudatosság:
   - felelős szakterület: IBF, együttműködve az Informatikai Igazgatósággal
   - feladat: az IBF évente és szükség esetén információbiztonsági oktatásokat szervez, amelynek célja a munkatársak tudatosságának növelése és az aktuális fenyegetettségek megismertetése. Az Informatikai Igazgatóság támogatást nyújthat a képzések szervezésében és technikai lebonyolításában;
e) Incidenskezelési folyamatok:
   - felelős szakterület: IBF, együttműködve az Informatikai Igazgatósággal
   - feladat: az IBF kialakítja és rendszeresen felülvizsgálja az incidenskezelési folyamatokat, biztosítva, hogy a biztonsági eseményeket gyorsan és hatékonyan kezeljék. Az Informatikai Igazgatóság részt vesz a technikai támogatásban és szükség esetén közreműködik a helyreállításban;
f) Auditok és felülvizsgálatok:
   - felelős szakterület: IBF, együttműködve az Informatikai Igazgatósággal
   - feladat: az IBF évente auditokat és felülvizsgálatokat végez az információbiztonsági intézkedések hatékonyságának értékelésére, az Informatikai Igazgatóság segítséget nyújt az auditok technikai előkészítésében és az eredmények elemzésében.

(4) A teljes körűségre vonatkozó alapelvet a fizikai, a logikai, az adminisztratív és a humán védelem területén kell érvényesíteni:
a) az összes információbiztonsági rendszerelem csoportra;
b) az informatikai szolgáltatás infrastrukturális környezetére;
c) a hardver rendszerre;
d) az alap és felhasználói szoftver rendszerre;
e) a kommunikációs és hálózati rendszerre;
f) az adathordozókra;
g) a dokumentumokra és feljegyzésekre;
h) az egyetemi polgárokra és a külső partnerekre;
i) a nemzetközi és magyar szabványban meghatározott nyílt rendszerek architektúrájának minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén.

(5) A szabályzatokat közzététel útján megismerhetővé kell tenni, az új belépőket oktatásban kell részesíteni, szükség esetén további képzéseket kell szervezni.

Az információbiztonsági szabályozás rendszere

**7. §** (1) Az informatikai biztonsági rendszer kiépítése során az Egyetem elkötelezi magát a folyamatszemléletű működés mellett. Az informatikai rendszer kialakítása és működtetése a PDCA (Plan-Do-Check-Act) modellnek megfelelően valósul meg. Ezt támogatja és erősíti a kockázatalapú gondolkodásmód, mely elősegíti a követelményeknek való megfelelés mellett az átgondolt folyamatok kialakítását, nyomon követését és szükség szerinti korrigálását is.

(2) Jelen Szabályzat az informatikai biztonság alapdokumentuma, mely magas szinten, keretjelleggel szabályozza az információbiztonsági szempontból releváns területeket a 2. számú mellékletben felsorolt jogszabályi előírásoknak megfelelően.
A Szabályzat tartalmazza az információbiztonsági alapelveket, az információbiztonsági irányítási rendszer kereteit, és meghatározza a legfontosabb követelményeket és elvárásokat.
Az információbiztonsági szempontból releváns területek közé tartozik a hozzáférés-kezelés, adatvédelem, incidenskezelés, rendszerbiztonság, fizikai biztonság, és a folyamatos működés biztosítása.

A jogszabályi előírások és szabványok, (pl.: a NIS2 irányelv) és más releváns szabályozások beépítésre kerülnek a Szabályzatba, biztosítva, hogy az Egyetem információbiztonsági gyakorlatai megfeleljenek a nemzeti és nemzetközi követelményeknek.

(3) A folyamatleírásokat, a dokumentációs mintákat, valamint a dokumentációkkal szemben támasztott informatikai szakmai követelményeket, elvárásokat az Információbiztonsági szakterület a saját elektronikus felületén, továbbá amennyiben az adattartalom felhasználói jogosultsághoz kötött, nem nyilvános dokumentumtárában tárolja és teszi elérhetővé az Informatikai Igazgatóság munkatársai és az érintettek adatgazdák számára.
Az Információbiztonsági szakterület vezetését ellátó IBF felelős a részletes folyamatleírások kidolgozásáért, amelyek magukban foglalják az információbiztonsági eljárások lépéseit, a feladatokat, felelősségeket és a kapcsolódó dokumentációs követelményeket.
Az informatikai szakmai követelmények meghatározzák a dokumentációs formátumokat, a tartalmi elemeket, és az információbiztonsági intézkedések megfelelőségi kritériumait.
Az elektronikus felületeken és nem nyilvános dokumentumtárakban tárolt dokumentumokhoz való hozzáférést szigorúan szabályozzák, biztosítva, hogy csak az arra jogosult munkatársak és adatgazdák férhessenek hozzájuk.

(4) Az egyes elektronikus információs rendszerekre vonatkozó különleges szabályozásokat a rendszerspecifikus előírások és dokumentációk tartalmazzák a jelen Szabályzat által definiált alapelvek figyelembevétele mellett. Ezek a dokumentációk biztosítják, hogy az egyes rendszerek speciális biztonsági követelményei is megfelelően kezelve legyenek.
A rendszerspecifikus előírások tartalmazzák az adott informatikai rendszerre vonatkozó részletes biztonsági követelményeket, beleértve a hozzáférés-kezelést, adatvédelmet, incidenskezelést, és a rendszerbiztonságot.
Ezek a dokumentációk biztosítják, hogy minden informatikai rendszer sajátos biztonsági kihívásai és kockázatai megfelelően kezelve legyenek, figyelembe véve az adott rendszer jellemzőit és működési környezetét.
Az előírások rendszeres felülvizsgálatával és frissítésével biztosítják, hogy azok mindig naprakészek és hatékonyak legyenek az új fenyegetések és kockázatok kezelésében.

(5) A rendszerspecifikus előírások és dokumentációk kiadása és módosítása előtt az Informatikai Igazgatóság igazgatója (továbbiakban: informatikai igazgató), köteles az IBF-nek, személyes adatok érintettsége esetén az adatvédelmi tisztviselőnek, valamint egészségügyi adatok érintettsége esetén az egészségügyi adatvédelmi tisztviselőnek a véleményét kikérni.

Információbiztonsági Politika

**8. §** (1) Az Egyetem az Információbiztonsági Politikában határozta meg az információbiztonsági működés kereteit, alapvető működésének elvét. Az Információbiztonsági Politika jelen Szabályzat 3. számú mellékletét képezi.

(2) Az Egyetem szervezeti egységei által kezelt informatikai infrastruktúra védelmét az adatgazdáknak úgy kell megvalósítaniuk, hogy az informatikai szolgáltatásoknak és környezetüknek védelme teljes körű, zárt, kockázatokkal arányos és folytonos legyen, valamint, hogy megvalósuljon a zárt szabályozási ciklus az Információbiztonsági Politikában leírtaknak, valamint a jelen Szabályzatban foglaltaknak megfelelően.

Információbiztonsági kockázatmenedzsment

**9. §** (1) A kockázatelemzés végrehajtásához az Egyetem 7/2023. számú kancellári utasításában meghatározottak alapján szükséges eljárni, mely tartalmazza a Pécsi Tudományegyetem belső kontrollrendszerének szabályait.

(2) Az információbiztonsági kockázatok felmérését az integrált kockázatfelmérés keretében kell elvégezni, felelőse az IBF.

Megelőző intézkedések rendszere

**10. §** (1) A megelőző intézkedések célja a nemkívánatos események megelőzése.

(2) A nemkívánatos események megelőzése érdekében az Egyetem a következő intézkedéseket alkalmazza:
a) informatikai technológiai védelmi intézkedéseket foganatosít annak érdekében, hogy a nagy gyakorisággal bekövetkező fenyegetésekből eredő kockázatok bekövetkezésének valószínűségét vagy bekövetkezésük esetén azok hatását csökkentse;
b) szabályozott folyamatokat vezet be, eljárásrendekben, munkautasításokban rögzíti a biztonsági kontrollok működtetését, illetve az esetleges incidensek feltárását és kezelését;
c) rendszeres biztonságtudatossági oktatásokat végez a humánkockázatok csökkentésére.

Biztonsági események kezelése

**11. §** (1) A biztonsági esemény kezelésének célja az információbiztonságot, a szervezet erőforrásainak, folyamatainak, információbiztonsági kontrolljainak működését veszélyeztető, illetve a rendeltetésszerűtől eltérő események figyelése, biztonsági események azonosítása, kezelése, valamint annak lezárását követően tanulságok levonása és védelmi intézkedések meghatározása a biztonsági esemény okának megszüntetésére a további bekövetkezési gyakoriság, illetve hatás csökkentése céljából. Az Egyetem biztonsági események kezelésének dokumentált kidolgozásáért az IBF és az informatikai rendszerek üzemeltetését és szolgáltatását nyújtó egyetemi informatikai igazgatóság szervezeti egységeinek vezetői felelnek.

(2) A biztonsági események kezelésének lépései a következők:
a) Felkészülés:
   - kidolgozni és dokumentálni az incidenskezelési terveket és eljárásokat,
   - kijelölni az incidenskezelésért felelős csapatot és biztosítani számukra a szükséges képzéseket és erőforrásokat.
b) Események azonosítása és észlelése:
   - implementálni kell a megfelelő eszközöket és technológiákat (például behatolásérzékelő rendszerek, naplózó eszközök), amelyek segítenek az események gyors észlelésében,
   - biztosítani kell a folyamatos monitoringot és naplózást az informatikai rendszerekben és hálózatokban.
c) Bejelentés:
   - létre kell hozni egy bejelentési csatornát, amelyen keresztül a dolgozók észlelhetik és jelenthetik a biztonsági eseményeket,
   - biztosítani kell, hogy minden dolgozó ismerje és kövesse a bejelentési eljárást.
d) Első válasz:
   - gyorsan reagálni a bejelentett eseményekre az incidenskezelési terv szerint,
   - azonnal megkezdeni az esemény korlátozását és izolálását annak érdekében, hogy minimalizáljuk a kárt és megakadályozzuk a további terjedést.
e) Elemzés és értékelés:
   - részletesen elemezni az eseményt, meghatározva annak okát, hatását és a sebezhetőségeket,
   - dokumentálni az esemény részleteit, beleértve az idővonalat, a használt eszközöket és technikákat.
f) Válaszintézkedések:
   - implementálni a megfelelő válaszintézkedéseket, amelyek magukban foglalhatják a rendszerek visszaállítását, a sebezhetőségek kijavítását és a sérült adatok helyreállítását,
   - értesíteni a megfelelő belső és külső érintetteket a helyzet súlyosságától és jellegétől függően.
g) Tanulás és fejlesztés:
   - az esemény utáni értékelést (post-incident review) végezni annak érdekében, hogy tanuljunk a történtekből,
   - az eseményből levont tanulságok alapján frissíteni és fejleszteni az incidenskezelési terveket és eljárásokat.
h) Dokumentáció és jelentés:

- részletes jelentést készíteni az eseményről, beleértve az okokat, hatásokat, a válaszintézkedéseket és a javasolt fejlesztéseket,
- az eseményeket és az azokkal kapcsolatos intézkedéseket nyilvántartásban rögzíteni az auditálhatóság és a jövőbeli referencia érdekében.

(3) A biztonsági események kezelése során együtt kell működni az érintett felekkel, beleértve a rendszergazdákat, a biztonsági szakértőket és a vezetést, biztosítva a hatékony kommunikációt és koordinációt.

Biztonsági esemény jelentése

**12. §** (1) A biztonsági eseményt az észlelőnek haladéktalanul jelenteni kell az észleléskor az Informatikai Igazgatóság által a honlapján közzétett elektronikus címen (biztonsági esemény bejelentő csatorna), illetve a biztonsági esemény bejelentése tehető közvetlenül az IBF-nek és az informatikai igazgatónak is. Amennyiben a biztonsági esemény személyes adatokat is érint és adatvédelmi incidens is megvalósul egyidejűleg az Adatvédelmi Tisztviselőt, illetve egészségügyi adatok érintettsége esetén az Egészségügyi Adatvédelmi Tisztviselőt is értesíteni szükséges az Egyetem adatvédelmi szabályzataiban foglaltaknak megfelelően.

(2) Biztonsági eseményre utalhat, melyet a felhasználóknak azonnal jelenteniük kell, ha
a) szolgáltatás, a berendezés vagy az eszközök elvesztése történik;
b) rendszer rendellenes működését észlelik;
c) a szabályzatoknak vagy irányelveknek való nem-megfelelés válik nyilvánvalóvá;
d) észlelhető a fizikai biztonsági rendelkezések megsértése;
e) nem ellenőrzött rendszerbeli változásokat tapasztalnak;
f) a szoftver vagy hardver hibás működése lép fel;
g) jogosulatlan hozzáférést tapasztalnak.

(3) Biztonsági eseménynek számít minden, 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.
Információbiztonsági incidens kezelése során törekedni kell arra, hogy bizonyítékok összegyűjtésre kerüljenek.

(4) Az értesítés rendet külön kancellári utasítás keretében – a biztonsági eseménykezelési eljárásrendben – szükséges részletesen meghatározni. Az esemény jelentésében szerepelnie kell a bejelentő nevét és elérhetőségeit is, hogy további információk szükségessége esetén kapcsolatba lehessen lépni vele.

(5) Amennyiben szükséges, a biztonsági eseményt a hatályos jogszabályok szerint jelenteni kell az illetékes hatóságok felé is, a vonatkozó jogszabályokban megkövetelt határidőn belül.

(6) A biztonsági esemény jelentésének elmulasztása az eseményjellegétől és mértékétől függően szankcionálható.

(7) Az Informatikai Igazgatóság arra kijelölt felelőseinek naponta ellenőriznie kell a naplóállományok bejegyzései alapján generált riasztásokat. A naplózási és naplóelemzési eljárásrend tartalmazza a jelentési folyamat leírását.

(8) Az informatikai biztonsági szabályok megsértését jelenteni kell a IBF-nek, PTE IT Ügyfélszolgálatának és az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály és Informatikai Alkalmazástámogatási és Fejlesztési Főosztály főosztályvezetőjének. Az IBF az Informatikai Igazgatóság igazgatójával közösen dönt a szabálysértés súlyának ismeretében a következményekről:
a) gondatlanságból elkövetett vagy szándékos, de enyhe szabálysértések esetén figyelmezteti a szabálysértőt és értesíti annak közvetlen felettesét a szabálysértésről;
b) ha a szabálysértés az Egyetem informatikai rendszerének működését sérti, vagy veszélyezteti,

- minősíti a szabálysértést a körülmények ismeretében, az érintettek bevonásával kivizsgálja a biztonsági eseményt.

(9) A biztonsági esemény kivizsgálásának eredményéről a vizsgálatban résztvevő személyek tájékoztatást adnak a Kancellárnak, aki dönt a további eljárásról.

(10) A biztonsági eseményekből levont tapasztalatokat folyamatosan értékelni kell, és azokat figyelembe kell venni a védelmi rendszer tervezése, szervezése, működtetése során.

(11) Az informatikai rendszerekkel összefüggő biztonsági események és gyengeségek kommunikálása olyan módon történjen, ami időben lehetővé teszi a szükséges helyesbítő intézkedések megtételét.

(12) A felhasználók tudatossági oktatásában ki kell térni arra, hogy hogyan kell válaszolniuk egy-egy felmerült biztonsági eseményre és milyen módon kell elősegíteniük a bizonyítékok gyűjtését.

(13) A részletszabályokat a Biztonsági esemény és incidenskezelési eljárásrend tartalmazza.

Nem megfelelőség és helyesbítő tevékenység

**13. §** (1) Helyesbítő tevékenységet kell folytatni biztonsági esemény bekövetkezése során. A megelőző vagy helyesbítő tevékenység révén biztosítható, hogy az információk védelmével kapcsolatos problémák gyorsan és eredményesen kiküszöbölhetők legyenek, a hasonló események bekövetkezési valószínűsége a jövőben csökkenjen. A megelőző és helyesbítő tevékenységek szisztematikus alkalmazásával az információk biztonságának folyamatos javulását érhetjük el.

(2) A megelőző és helyesbítő tevékenységeket általában az alábbi esetekben folytat az Egyetem:
a) felhasználók, vagy külső érdekelt felek (megbízó, tanácsadó, auditor, szakértő stb.) által jelzett információbiztonsággal kapcsolatos észrevételek esetén;
b) egyedi (olyan egyszeri események, amelyek komoly biztonsági kockázatot jelentenek) és ismétlődő (gyakran előforduló, rendszerszintű hibák) problémák esetén;
c) a rendszerrel kapcsolatos nem-megfelelőségek esetén (auditjelentés) melyek közé tartoznak az auditok során feltárt nem-megfelelőségek és hiányosságok, amelyek az információbiztonsági rendszer működésében észlelhetők.

(3) A megelőző és helyesbítő tevékenységek során azonosítani kell a problémát, fel kell tárni a hibák okait, a megszüntetésükre és ismételt előfordulásuk megakadályozására intézkedéseket kell kialakítani és bevezetni. A megelőző és helyesbítő intézkedések megvalósítását dokumentálni szükséges és eredményességét meghatározott időközönként mérni kell.

(4) Az Egyetem információbiztonsági rendszerében meghatározott szabályoktól való eltérést az IBF az informatikai igazgató egyetértésével kizárólag írásban, indokolással engedélyezheti. Az engedélyeket tartalmazó nyilvántartást az Információbiztonsági szakterület vezeti. Az engedélyezett eltéréseket rendszeres időközönként felül kell vizsgálni annak biztosítása érdekében, hogy továbbra is indokoltak és biztonságosak legyenek. A felülvizsgálatok eredményeit dokumentálni kell, és szükség esetén intézkedéseket kell hozni az eltérések megszüntetésére vagy módosítására.

Védelmi intézkedések módosítása

**14. §** (1) A védelmi intézkedések módosítása az Egyetem információbiztonsági rendszerének folyamatos fejlesztése érdekében történik. A védelmi intézkedések módosítását szükségessé teheti:
a) amennyiben a korábbi védelmi intézkedés szintje nem érte el a kívánt biztonsági szintet;
b) amennyiben az informatikai rendszer változása miatt a korábbi biztonsági kontrollok érvényüket vesztik;
c) amennyiben az adott kontroll elavul és/vagy jobb, újabb technológiák bevezetése válik indokolttá.

(2) Az informatikai rendszer rendszeres kockázatelemzése során feltárt hiányosságok vagy nem-megfelelőségek azt mutathatják, hogy a jelenlegi védelmi intézkedések nem biztosítanak megfelelő védelmet. Ilyen esetekben az intézkedések felülvizsgálatára és módosítására van szükség, hogy az információbiztonság szintje megfeleljen az elvárt követelményeknek. A biztonsági szint növelése érdekében konkrét javító intézkedéseket kell kidolgozni és bevezetni. Ez magában foglalhatja új technológiák alkalmazását, meglévő intézkedések módosítását vagy kiegészítő védelmi rétegek bevezetését.

(3) Az informatikai rendszer bármely változását, új szoftverek vagy hardverek bevezetését, folyamatosan nyomon kell követni. Minden változás esetén értékelni kell, hogy a meglévő biztonsági kontrollok továbbra is érvényesek-e, vagy szükséges-e azokat módosítani. Az új környezethez és technológiai feltételekhez igazodva frissíteni kell a biztonsági intézkedéseket. Ez magában foglalhatja új biztonsági protokollok bevezetését, meglévő kontrollok átalakítását vagy új intézkedések bevezetését.

(4) Az információbiztonság területén folyamatosan figyelemmel kell kísérni a technológiai fejlesztéseket és új innovációkat. Az elavult biztonsági intézkedéseket fel kell váltani korszerűbb, hatékonyabb megoldásokkal. A jobb technológiák bevezetésével kapcsolatos projektek keretében fel kell mérni a jelenlegi rendszer hiányosságait és kidolgozni a szükséges intézkedéseket az új technológiák integrálására és a biztonsági szint növelésére.

(5) A védelmi intézkedések módosításának folyamata:
a) Kockázatelemzés és értékelés: Minden módosítás előtt alapos kockázatelemzést kell végezni, amely feltárja a potenciális veszélyeket és meghatározza a szükséges védelmi szintet.
b) Tervezés és jóváhagyás: A módosítási javaslatokat részletes terv formájában kell kidolgozni és az informatikai igazgató, valamint az Információbiztonságért Felelős jóváhagyásával bevezetni.
c) Végrehajtás és dokumentálás: A jóváhagyott módosításokat be kell vezetni a rendszerbe, és a változtatásokat részletesen dokumentálni kell a nyomon követhetőség biztosítása érdekében.
d) Utólagos ellenőrzés és értékelés: A módosítások bevezetése után rendszeres időközönként ellenőrizni kell azok hatékonyságát és a védelmi szintet, biztosítva ezzel a folyamatos fejlődést és a biztonság fenntartását.

Biztonsági események lezárása

**15. §** (1) A biztonsági esemény kezelése abban az esetben tekinthető lezártnak, amennyiben a biztonsági eseményre való reagálás, elhárítás megtörtént, további károk okozása elhanyagolható, valamint a bizonyítékok gyűjtése és vizsgálata lezárult, az esemény teljes kivizsgálása lezárult, a szükséges megállapításokat a szakértők megtették és a kivizsgálás során levont következtetéseket és javasolt intézkedéseket írásban rögzítették.

(2) A biztonsági esemény vagy incidens elhárításának lépéseit, illetve kivizsgálásának eredményeit dokumentált módon rögzíteni kell. A dokumentáció formája lehet jegyzőkönyv, vagy valamely erre a célra alkalmazható informatikai rendszer is. A dokumentációnak tartalmaznia kell az esemény leírását, beleértve a bekövetkezés időpontját, helyét és a résztvevő rendszereket, az elhárítási intézkedések részletes leírását, az összegyűjtött bizonyítékok listáját és azok elemzésének eredményeit, valamint a szakértők által levont következtetéseket és javasolt további intézkedéseket.

(3) A biztonsági esemény vagy incidens elhárításáról írásban (elektronikus levél, belső portálon tájékoztatás, felugró ablak) tájékoztatni kell az elhárításban, illetve kivizsgálásban résztvevőket, valamint az érintett munkatársakat. A tájékoztató csak a szükséges és elégséges mértékben kell, hogy tartalmazza az információkat, az események, illetve vizsgálati eredmények részletes megosztása tilos. A tájékoztatónak magában kell foglalnia az esemény rövid leírását, az elhárítási intézkedések összefoglalását, a kivizsgálás eredményeinek lényegét, anélkül, hogy érzékeny vagy részletes adatokat osztana meg, valamint az érintettek további teendőit és javaslatokat a hasonló események megelőzésére.

(4) Az esemény lezárását követően rendszeres időközönként felül kell vizsgálni az elhárítási intézkedések hatékonyságát és az események kezelésének folyamatát. Az eseményekből levont tanulságok alapján javító

intézkedéseket kell bevezetni az információbiztonsági rendszer folyamatos fejlesztése érdekében. Ezek az intézkedések lehetnek új technológiák és védelmi intézkedések bevezetése, az eljárások és protokollok módosítása és finomítása, képzési és tudatosságnövelő programok indítása az érintett munkatársak számára.

(5) A biztonsági eseményekről és azok kezeléséről részletes jelentéseket kell készíteni, amelyek tartalmazzák a történések, az elhárítási lépések és a kivizsgálás eredményeit. Ezeket a jelentéseket meg kell osztani az illetékes vezetőkkel és hatóságokkal.

Tanulás a biztonsági eseményekből

**16. §** (1) Az IBF feladata az informatikai igazgató által meghatározott munkatársak bevonásával a biztonsági események során keletkező kár mértékének meghatározása, valamint a biztonsági események során nyert tapasztalatok felhasználásával a meglévő információbiztonsági rendszer tökéletesítése.

(2) A biztonsági esemény ismételt előfordulásának megakadályozása érdekében az IBF a szükséges szakértők bevonásával intézkedési tervet kell kidolgoznia. Az intézkedési tervnek tartalmaznia kell a biztonsági esemény okainak részletes leírását, az események megelőzését célzó konkrét intézkedéseket és javaslatokat, az intézkedések végrehajtásának ütemtervét és felelőseit, valamint a megelőző intézkedések hatékonyságának mérési módszereit. Az intézkedési tervet az informatikai igazgató véleményezi.

(3) Az intézkedési tervek végrehajtásáról szóló jelentésekben az IBF beszámol a Kancellárnak a biztonsági eseményekről, incidensekről, a kidolgozott és végrehajtott akciótervekről.

A szervezet biztonsági szintbe és az elektronikus információs rendszerek biztonsági osztályba sorolása

**17. §** (1) A rendszerhez rendelt védelmi intézkedések tervezése és teljesítése az elektronikus információs rendszerek 2. számú mellékletben felsorolt jogszabályi előírásoknak, követelményeknek megfelelően és a hatályos jogszabályban előírtak alapján történik. A védelmi intézkedések kidolgozása során figyelembe kell venni a rendszer specifikus biztonsági követelményeit, beleértve az adatvédelem és adatbiztonság szempontjából kritikus területek azonosítását, a rendszer működését és integritását fenyegető kockázatok elemzését, valamint a megfelelő technológiai és adminisztratív védelmi intézkedések meghatározását és bevezetését.

(2) Az Ibtv. alapján a szervezet biztonsági szintjét és az elektronikus információs rendszerek biztonsági osztályba sorolását az IBF javaslatára a Kancellár határozza meg. Az elektronikus információs rendszerek besorolását az 4. számú melléklet, az Egyetem aktuális biztonsági szintjét a 5. számú melléklet tartalmazza. Az elektronikus információs rendszerek biztonsági osztályba sorolása során figyelembe kell venni a rendszer által kezelt adatok érzékenységét és fontosságát, a rendszer működésének kritikus jelentőségét az Egyetem működésére nézve a rendszer biztonsági követelményeit és az elérni kívánt biztonsági szintet.

(3) Amennyiben egy, az Ibtv. hatálya alá tartozó információs rendszernél az elvárt biztonsági szint nem teljesül, a szervezetnek két évente szükséges legalább egy fokozattal magasabb biztonsági szintet elérnie mindaddig, amíg az elvárt szint nem teljesül. A magasabb szint elérése érdekében két évre vonatkozóan cselekvési tervek kidolgozása szükséges, melyek megvalósítása az IBF jóváhagyását követően kezdhető meg. A cselekvési tervek végrehajtása során folyamatosan ellenőrizni kell a biztonsági szint elérésének ütemezését és a bevezetett intézkedések hatékonyságát.

(4) Az IBF gondoskodik a rendszerek osztályba sorolásának háromévenkénti vagy szükség esetén soron kívüli felülvizsgálatáról. A biztonsági szintbe sorolás eredményét jelen szabályzat 5. számú mellékletében kell rögzíteni. Új rendszer bevezetésekor annak biztonsági osztályba sorolása is megtörténik és meghatározásra kerülnek az osztály követelményeinek teljesítéséhez szükséges intézkedések.

(5) A dokumentációnak a következő elemeket kell tartalmazni:

a) Bevezetés: Rövid összefoglaló a felülvizsgálat céljáról, amely magában foglalja a felülvizsgálat szükségességének indoklását és a felülvizsgálat hatókörének meghatározását. Az időszak meghatározása, amelyet a felülvizsgálat átfog, beleértve az előző felülvizsgálat óta eltelt időt.
b) Felülvizsgálati módszertan: Az alkalmazott módszerek és technikák részletes leírása, például interjúk, kérdőívek, rendszerellenőrzések, tesztek és kockázatelemzések. Azoknak a szakértőknek és munkatársaknak a listája, akik részt vettek a felülvizsgálatban, valamint az általuk ellátott szerepkörök és feladatok.
c) Jelenlegi helyzet elemzése: Az információbiztonsági rendszer jelenlegi állapotának részletes leírása, beleértve az alkalmazott technológiákat, folyamatokat és védelmi intézkedéseket. Az aktuális biztonsági szint részletes értékelése, amely magában foglalja az egyes rendszerek biztonsági osztályba sorolását és azok megfelelőségét a jogszabályi előírásoknak.
d) Kockázatelemzés: A felülvizsgálat során azonosított kockázatok részletes leírása, beleértve a kockázatok forrását és potenciális hatását. Az azonosított kockázatok értékelése, beleértve a valószínűségi és hatás alapú kockázati besorolást.
e) Események és incidensek elemzése: Az előző felülvizsgálat óta bekövetkezett biztonsági események és incidensek részletes elemzése, beleértve azok okait, következményeit és az elhárításukra tett intézkedéseket. Az eseményekből levont tanulságok és azok hatása a jelenlegi biztonsági intézkedésekre és folyamatokra.
f) Megelőző és helyesbítő intézkedések: Az előző felülvizsgálat óta végrehajtott megelőző és helyesbítő intézkedések részletes leírása, beleértve az intézkedések hatékonyságát és eredményességét. Az újonnan javasolt megelőző és helyesbítő intézkedések, amelyek a felülvizsgálat eredményeként kerültek azonosításra.
g) Fejlesztési javaslatok: A biztonsági rendszer fejlesztésére vonatkozó javaslatok, beleértve a technológiai és folyamatbeli fejlesztéseket. Javaslatok a biztonságtudatosság növelésére és a munkatársak képzésére vonatkozóan.
h) Megvalósítási ütemterv: A javasolt intézkedések megvalósításának részletes ütemezése, beleértve a prioritási sorrendet és a végrehajtás határidejét. Az egyes intézkedések végrehajtásáért felelős személyek és csoportok meghatározása.
i) Felügyelet és jelentéstétel: A biztonsági intézkedések megvalósításának és hatékonyságának nyomon követésére szolgáló felügyeleti mechanizmusok leírása. A jelentéstétel követelményei, beleértve a jelentések gyakoriságát és tartalmát.
j) Dokumentáció és nyilvántartás: A felülvizsgálat során készített jegyzőkönyvek és azok tartalma. A kockázatelemzések és eseményvizsgálatok eredményeinek részletes dokumentálása. A javasolt és végrehajtott intézkedési tervek részletes dokumentációja. Az összes kapcsolódó nyilvántartás és azok rendszeres frissítése.

## 3. fejezet Az információbiztonság szervezete

Információbiztonsági szerepkörök

**18. §** (1) Az informatikai és az információbiztonsági feladatokat ellátó és az információbiztonság koordinálásában szerepet játszó szervezeti egységeket szervezeti szinten el kell különíteni a Pécsi Tudományegyetem Szervezeti és Működési Szabályzatában, valamint a kapcsolódó mellékleteiben. Az elkülönítés biztosítja, hogy az információbiztonsági funkciók és a napi informatikai működés ne ütközzenek, és megfelelő függetlenséggel rendelkezzenek a hatékony működés érdekében.

(2) Az Egyetem információbiztonsági rendszerének működtetése a Kancellár feladata, tevékenységét az IBF útján gyakorolja. E Szabályzatban meghatározott intézkedési jogköröket a Kancellár által más személyek, szervezeti egységek részére átruházott hatáskörként kell értelmezni.

(3) Az informatikai szerepkörök és feladatok szervezeti egységre és személyre telepítését úgy kell végrehajtani, hogy a fejlesztési, üzemeltetési, ellenőrzési feladatok ellátásának egymástól való függetlensége biztosított legyen.

(4) Az informatikai és az informatikai biztonsági szerepkörök és feladatok kiosztásakor a közvetlen vezető köteles gondoskodni a helyettesítésről. Helyettesítési tervek biztosítják, hogy az információbiztonsági funkciók folyamatosan elláthatók legyenek, még a kulcsfontosságú személyzet távolléte esetén is.

(5) Az Egyetemnek rendszeres képzéseket és tudatosságnövelő programokat kell biztosítania minden munkatárs számára az információbiztonsági politikák és eljárások megértése és betartása érdekében. Különös figyelmet kell fordítani a kulcsfontosságú információbiztonsági szerepköröket betöltő személyzet szakmai fejlesztésére.

(6) Az Egyetemnek rendszeres időközönként kockázatelemzést kell végeznie az információbiztonsági kockázatok azonosítása és kezelése érdekében. Az eredményeket dokumentálni kell, és azokat a vezetés rendszeresen felülvizsgálja. Az információbiztonsági rendszernek meg kell felelnie a vonatkozó jogszabályi és szabályozási követelményeknek, ideértve a NIS2 irányelvet is.

(7) Az Egyetemnek kialakított, dokumentált és évente tesztelt incidenskezelési tervvel kell rendelkeznie. Az incidenskezelési tervnek tartalmaznia kell a biztonsági események észlelésének, bejelentésének, kezelésének és felülvizsgálatának lépéseit.

(8) Az Egyetem rendszeresen, de legalább évente belső és külső auditokat végez az információbiztonsági rendszer megfelelőségének és hatékonyságának értékelése érdekében. Az auditok eredményeit dokumentálni kell, és a vezetés részére jelentést kell készíteni az esetleges hiányosságok és javító intézkedések megvitatása céljából.

Adatgazdai szabályozás

**19. §** (1) Az Adatgazdák feladata az Egyetem adatvagyona tekintetében, hogy a jogszabályban és az egyetemi szabályzók által megfogalmazott biztonsági követelményeket érvényesítsék. Ez magában foglalja az adatbiztonság, adatvédelem és adatkezelési elvek alkalmazását, biztosítva az adatok sértetlenségét, rendelkezésre állását és bizalmasságát. Az adatok kezelésével kapcsolatos felelősségek az adatokat ténylegesen felhasználó szervezeti egységekre hárulnak, azonban az adatgazdák feladata, hogy ezeket a követelményeket felügyeljék és betartsák.

(2) Adatgazda a végső felelőse egy bizonyos adathalmaz jelentésének, tartalmának, minőségének, biztonságának és elérhetővé tételének, ideértve azt is, hogy az adatot hogyan definiálják, hogyan állítják elő, hogyan azonosítják, hogyan tartják karban, hogyan használják fel. A PTE szervezeti egységeinél kezelt adatok tekintetében adatgazda, aki felelős a szervezeti egysége által kezelt valamennyi adat IBSZ-nek megfelelő kezelésért. Az Adatgazda kijelölésének lépései:

a) Azonosítás: azonosítani szükséges a szervezet kritikus rendszereit és adatait, valamint az ezekhez kapcsolódó kockázatokat, mely tevékenység magában foglalja a kockázatelemzést és a sebezhetőségek feltárását.
b) Szerepkörök meghatározása: definiálni szükséges az adatgazda szerepkörét, feladatait és felelősségi köreit, melyet dokumentálni kell a szervezet biztonsági politikájában.
c) Kijelölés: szervezeti egységek vezetői kijelölik az adatgazdákat, melyet követően az adatgazda felelős az adott rendszerekért és adatokért azzal, hogy az adatgazdáknak rendelkezniük kell a szükséges szakértelemmel és erőforrásokkal.
d) Képzés és támogatás: biztosítani kell, hogy az adatgazdák megfelelő képzést és támogatást kapjanak feladataik ellátásához, mely magában foglalja a szakmai továbbképzéseket és a szükséges eszközök biztosítását.
e) Felügyelet és auditálás: rendszeresen ellenőrizni és auditálni kell az adatgazdák munkáját, hogy biztosítani lehessen a szabályozásoknak való megfelelést; az auditálás magában foglalja a folyamatok és intézkedések felülvizsgálatát, valamint a megfelelés ellenőrzését.

(3) Az adatgazda feladatai közé tartozik:

a) az adatkörök meghatározása.
b) az adatok biztonsági osztályba sorolása

c) az adatok rendelkezésre állásának biztosítása (az adatok elérhetőségének garantálása az arra jogosult felhasználók számára).

(4) Minden lépést és folyamatot dokumentálni kell, hogy átlátható és visszakövethető legyen a megfelelés. Ez magában foglalja az adatgazdák kijelölését, a kockázatelemzési jelentéseket, az incidensjelentéseket és a képzési anyagokat.

(5) Hatékony kommunikációs csatornákat kell létrehozni az adatgazdák és a szervezet többi része között annak érdekében, hogy a biztonsági információk és események gyorsan és hatékonyan elérjenek minden érintetthez. Ez magában foglalja a rendszeres jelentéseket, a belső értekezleteket és a sürgősségi kommunikációs protokollokat.

(6) Minden adatgazdának el kell végeznie és legalább kétévente felül kell vizsgálnia az adatok biztonsági besorolását. Az adatgazdáknak a hozzájuk tartozó adatkörök nyilvántartásba vételekor, illetve módosulásakor az Adatosztályozó lapot (6. számú melléklet – Adatosztályozó lap), illetve annak tartalmával megegyező nyilvántartást kell küldenie az Információbiztonság Felelősnek.

Külső ügyfelek és partnerek

Általános szabályok

**20. §** (1) Az információbiztonsági szabályozás szempontjából külső közreműködőnek, (a továbbiakban: harmadik félnek) tekintendő minden olyan külső szervezet, hatóság, szerződéses partner (jogi vagy természetes személy), akinek tevékenysége indokolttá teszi az Egyetem belső használatú és annál magasabb minősítésű adataihoz vagy bármely informatikai rendszeréhez történő hozzáférést.

(2) Kiemelt figyelmet kell fordítani a harmadik fél tevékenységében rejlő kockázatok azonosítására és kezelésére, beleértve az információbiztonsági követelmények betartását.

Harmadik féllel kötött titoktartási megállapodások

**21.§** (1) Az Egyetem informatikai rendszereit, szolgáltatásait használó harmadik fél vonatkozó szerződésében szerepelnie kell titoktartási záradéknak vagy titokvédelmi megállapodásnak, melyben a harmadik fél kötelezettséget vállal arra, hogy az Egyetem által biztosított összes adatot és információt, beleértve a személyes adatokat, szellemi tulajdonokat és üzleti titkokat, szigorúan bizalmasan kezeli, és azokat kizárólag a szerződéses kötelezettségek teljesítése érdekében használhatja fel; továbbá olyan záradékra, amely vagy tartalmazza, vagy utal minden olyan információbiztonsági követelményre, amely biztosítja az Szabályzatnak és az Egyetemen bevezetett szabályoknak való megfelelést. A szerződésben egyértelműen jelölni szükséges, hogy a harmadik fél tevékenységét ki felügyeli. A partner köteles megfelelő technikai, fizikai és szervezeti intézkedéseket hozni az Egyetem adatainak bizalmasságának, integritásának és rendelkezésre állásának védelme érdekében, az iparági legjobb gyakorlatokkal és a vonatkozó jogszabályokkal összhangban.

(2) Minden harmadik féllel kötött megállapodás esetében a megállapodásban rögzíteni kell az adatvédelmi és informatikai biztonsági kérdéseket. Személyes adatokhoz való hozzáférés vagy személyes adatok átadása kizárólag erre vonatkozó írásos szerződés (adatfeldolgozói megállapodás, közös adatkezelői megállapodás vagy az adattovábbítást szabályozó rendelkezések) alapján lehetséges. Az adatfeldolgozói megállapodásra az Egyetem Adatvédelmi Szabályzatának 4. §-a alkalmazandó.

(3) A jogszabályi előíráson alapuló, rendszeres vagy eseti adatszolgáltatások esetén, minden esetben meg kell győződni az adatközlés jogalapjáról, kétség esetén az adatvédelmi tisztviselő vagy egészségügyi adatok esetén az egészségügyi adatvédelmi tisztviselő közreműködését kell kérni. Adatot továbbítani csak abban az esetben lehet, ha annak jogalapja egyértelmű, célja, és az adattovábbítás címzettjének személye pontosan meghatározott.

(4) Az informatikai beszerzések vonatkozásában a Pécsi Tudományegyetem hatályos szabályzatai és vezetői utasításai alapján kell eljárni az információbiztonsági előírások betartása mellett.

A külső partnerekkel történő kapcsolattartás szabályai

**22. §** (1) Külső partnerek egyetemi informatikai szolgáltatásokhoz történő hozzáférését a 7/2017. számú kancellári utasítás szabályozza.

(2) A kapcsolattartó információbiztonsági kérdésekben elsősorban az IBF-től, továbbá az informatikai igazgatótól, valamint a személyes adatok védelmével kapcsolatos kérdésekben az egyetemi adatvédelmi tisztviselőtől, egészségügyi adatok esetén az egészségügyi adatvédelmi tisztviselőtől tájékoztatást vagy állásfoglalást kérhet.

(3) A személyes adatok vonatkozásában a Pécsi Tudományegyetem Adatvédelmi Szabályzata, míg az egészségügyi adatok kapcsán a Pécsi Tudományegyetem Egészségügyi Adatvédelmi Szabályzata az irányadó.

Ellenőrzések, monitorozás

**23. §** (1) A jelen fejezetben rögzített, harmadik félre vonatkozó információbiztonsági előírásokat az IBF a jelen Szabályzatban rögzítettek szerint köteles ellenőrizni.

(2) A harmadik féllel kötött szerződésben biztosítani kell az ellenőrzés Informatikai Biztonsági Felelős által történő elvégzésének lehetőségét.

(3) A harmadik fél által nyújtott szolgáltatások színvonalát monitorozni kell és vizsgálat keretében ellenőrizni szükséges, hogy a szerződésben előírt biztonsági előírások és egyéb szabályok betartásra kerülnek.

A harmadik fél által nyújtott szolgáltatások változásainak kezelése

**24. §** A harmadik féllel kötött szerződésben megkövetelt és bevezetett biztonsági intézkedések – beleértve a szabályzatokat, eljárásokat is – változásainak kezelésére olyan eljárásokat kell kidolgozni, melyek figyelembe veszik a folyamatok és rendszerek kritikusságát, az információbiztonsági előírások betartását, valamint biztosítják a kockázatok újraértékelését.

A harmadik féllel kötött megállapodások információbiztonsági követelményei

**25. §** (1) A jelen Szabályzat hatálya alá tartozó szerződéseknek lehetőség szerint ki kell térnie az alábbi információbiztonsági követelmények és elvárások meghatározására:

a) az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzési követelményeit, a külső szereplőkre vonatkozó általános információbiztonsági előírásokat;
b) az elektronikus levelezés, fájlok titkosításának szabályait;
c) a papír alapú dokumentumok kezelésének információbiztonsági szabályait;
d) amennyiben értelmezhető:
   - a látogatókra vonatkozó fizikai biztonsági szabályokat,
   - a hozzáférés módját az egyetemi IT- és információs rendszerekhez, a hozzáférés szabályait és a felhasználó felelősségeit,
   - a dokumentumok és adathordozók átadásának, cseréjének és kezelésének információbiztonsági követelményeit és az ezzel kapcsolatos felhasználói felelősségeket;
e) a szerződésben foglalt információbiztonsági követelmények megszegéséből származó szankciókat;
f) a harmadik félnél történő személyi változások kezelését;
g) a szerződés megszűnésekor vagy lejártakor az információk és átadott információhordozók visszaadásának, valamint a szerződéses partner adathordozóján lévő információk megsemmisítésének

követelményeit.

(2) A partnernek be kell vezetnie és fenntartania egy Információbiztonsági Irányítási Rendszert (ISMS), amely megfelel az iparágban elismert szabványoknak.

(3) A partner köteles rendszeresen értékelni és csökkenteni az Egyetem adatai biztonságát érintő kockázatokat, beleértve a kiberfenyegetések, emberi hibák és természeti katasztrófák okozta kockázatokat.

(4) A partner köteles szigorú hozzáférés-ellenőrzési intézkedéseket bevezetni, mint például a többfaktoros hitelesítés és a legkisebb jogosultság elve, biztosítva, hogy csak az arra felhatalmazott személyek férhessenek hozzá az Egyetem adataihoz.

(5) A partner köteles részletes naplókat vezetni az adatokhoz való hozzáférésről, és ezeket kérésre az Egyetem rendelkezésére bocsátani ellenőrzési célból.

(6) A partnernek kötelessége egy incidens-válaszadási tervet fenntartani, amely lehetővé teszi a biztonsági incidensek és adatsértések gyors észlelését, kezelését és mérséklését.

(7) A partnernek azonnal értesítenie kell az Egyetemet minden tényleges vagy gyanított biztonsági incidensről, adatvédelmi incidensről vagy jogosulatlan hozzáférésről az Egyetem rendszereihez, legfeljebb 24 órán belül.

(8) Amennyiben a partner alvállalkozókat vesz igénybe, azok kötelesek ugyanazon biztonsági követelményeknek és kötelezettségeknek megfelelni, mint amelyeket a partnerrel szemben támasztanak.

(9) A partner köteles rendszeres képzéseket szervezni munkavállalói számára az Információbiztonság témakörében, hogy növelje a tudatosságot és csökkentse a potenciális kockázatokat. A képzésnek ki kell terjednie a legfrissebb fenyegetésekre és a legjobb gyakorlatokra.

(10) A rendszer és szolgáltatás beszerzésekre, valamint a fejlesztésekre vonatkozó részletes informatikai biztonsági követelményeket és szabályokat az „Informatikai beszerzési eljárásrend” és a „Biztonságos fejlesztési követelmények eljárásrend” tartalmazza.

## 4. fejezet Az információ védelme, részletes védelmi intézkedések meghatározása

Részletes védelmi intézkedések minimum követelményei

**26. §** Annak érdekében, hogy az információ védelme egységesen legyen kezelve az Egyetemen belül, és a szükséges és elégséges információbiztonsági követelmények, kontrollok meghatározhatóak legyenek, legalább az alábbiak végrehajtása szükséges:

a) adatvagyon felmérés: minden információs eszköz (adatbázisok, fájlok, dokumentumok) azonosítása és nyilvántartásba vétele, az információs eszközök bizalmasság, sértetlenség és rendelkezésre állás alapján történő kategorizálása, minden információs eszközhöz felelős személy (adatgazda) kijelölése, aki felügyeli az eszköz védelmét és használatát;
b) üzleti hatáselemzés készítése: az Egyetem minden üzleti folyamatának azonosítása és dokumentálása, az egyes üzleti folyamatok kritikus fontosságú részeinek meghatározása, amelyek nélkülözhetetlenek az Egyetem működéséhez. annak elemzése, hogy az információs eszközök sérülése vagy elvesztése hogyan befolyásolja a kritikus üzleti folyamatokat;
c) kockázatelemzés készítése: az információbiztonságot veszélyeztető fenyegetések és sebezhetőségek azonosítása. A fenyegetések valószínűségének és a lehetséges következmények súlyosságának értékelése. Intézkedések meghatározása a kockázatok elfogadható szintre csökkentésére, ideértve a megelőző, észlelő és elhárító kontrollokat;
d) informatikai rendszerek biztonsági osztályba sorolása: az informatikai rendszerek biztonsági osztályokba sorolása a biztonsági követelmények és a kockázatelemzés eredményei alapján. A különböző osztályokhoz tartozó védelmi szintek és kontrollok részletes meghatározása. Az osztályozási rendszer rendszeres felülvizsgálata és szükség esetén frissítése a technológiai változások és új fenyegetések tükrében;

e) hozzáférés és jogosultság menedzsment folyamatok működtetése: hozzáférési jogosultságok meghatározása az információs eszközökhöz, szerepkörök és felelősségek alapján. Megfelelő azonosítási és hitelesítési mechanizmusok bevezetése, például jelszavak, biometrikus azonosítás, kétfaktoros hitelesítés. Az információs eszközökhöz való hozzáférés nyomon követése és rendszeres auditálása a jogosulatlan hozzáférés megelőzése érdekében;
f) adatvagyon elemek személyes, illetve egészségügyi adatköri minősítése: az adatvagyon elemeinek személyes adatok, egészségügyi adatok és egyéb érzékeny adatok alapján történő kategorizálása. A személyes és egészségügyi adatok kezelésére vonatkozó törvényi és szabályozási követelmények beépítése az adatkezelési folyamatokba. Megfelelő titkosítási és anonimizálási eljárások bevezetése az érzékeny adatok védelme érdekében.

Emberi erőforrásokkal kapcsolatos biztonsági intézkedések

**27. §** (1) A részletszabályokat a foglalkoztatott munkavégzésre irányuló jogviszonyának létesítése, megszűnése, valamint munkakörváltozása esetén érvényes eljárásrendje tartalmazza.

(2) Minden foglalkoztatottnak belépéskor alá kell írni a Titoktartási nyilatkozatot.

(3) Az Egyetem foglalkoztatottjaival a munkáltatói jogkör gyakorlójának meg kell ismertetnie az Informatikai Biztonsági Szabályzat munkakörük alapján rájuk vonatkozó szabályait:
a) az alkalmazandó információbiztonsági szabályokat;
b) az informatikai rendszerek használatával kapcsolatosan elvárt és tiltott magatartásokat, azok megsértésének szankcióit; ennek keretében a helyes és helytelen informatikai rendszerhasználat részletes bemutatását és az információbiztonsági szabályok megszegésének lehetséges következményeit, beleértve a fegyelmi és jogi szankciókat;
c) az informatikai rendszer számára nagy kockázattal járó fenyegetések és veszélyforrások közérthető magyarázatát, a biztonságtudatosság fokozása érdekében, így különösen a leggyakoribb fenyegetések (pl. phishing, malware) ismertetését és azok hatásainak bemutatását.

Általános információbiztonsági előírások a munkavégzés során

**28. §** (1) Minden esetben törekedni kell az „Üres íróasztal, tiszta képernyő” politika betartására, a munkanap végén irat nem maradhat az asztalokon, illetve a munkakörnyezetben.

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

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

Áthelyezésnél, munkavégzésre irányuló jogviszony megszűnésénél informatikai eszközök visszaszolgáltatása

**29. §** (1) Valamennyi foglalkoztatottnak és minden, az Egyetem informatikai rendszereit, szolgáltatásait használó harmadik félnek vissza kell szolgáltatnia az Egyetem valamennyi, használatra átvett informatikai vagyontárgyát, amikor foglalkoztatása, szerződése, megállapodása lejár vagy megszűnik. A visszaszolgáltatás azon szervezeti egység részére történik, ahol a vagyontárgy nyilvántartásba vétele korábban megtörtént.

(2) Az Informatikai Igazgatóság az eszköz leadásakor ellenőrzi az átvett és az Átadás-átvételi lapon rögzített hardver-, szoftver specifikáció meglétét és üzemképes állapotát. Az Informatikai Igazgatóság feladata, hogy az informatikai vagyontárgyak visszaszolgáltatását követően gondoskodjon azok alaphelyzetbe állításáról, amely magában foglalja az eszközök adatainak biztonságos törlését és az eredeti gyári vagy vállalati beállítások visszaállítását. Ezt követően az Informatikai Igazgatóság biztosítja az eszközök újbóli hasznosítását (amennyiben használható még), ami lehetőséget nyújt arra, hogy a vagyontárgyakat nyilvántartásba vétel szerinti szervezeti egységek vagy felhasználók számára megfelelő állapotban, a vonatkozó biztonsági előírásoknak és belső szabályzatoknak megfelelően ismételten rendelkezésre bocsássák. Ez alól kivételt képez

a Klinikai Központ nyilvántartásába tartozó eszközök visszavétele, melyek esetében az Egészségügyi Gazdálkodási Igazgatóság végzi az ellenőrzést.

Információbiztonsági oktatás és képzés, az információbiztonsági tudatosság elérése

**30. §** (1) A biztonságtudatossági oktatás célja, hogy az Egyetemen foglalkoztatottak értesüljenek a rájuk vonatkozó, Egyetem által előírt szabályozásokról, biztonsági előírásokról, tisztában legyenek azok betartásának szükségességével, tudomást szerezzenek az őket fenyegető lehetséges veszélyekről, támadási technikákról és elhárításukról, észlelésükről és jelentési módjukról.

(2) Az Egyetem informatikai rendszerei felhasználóinak a munkakörükhöz igazodó informatikai és információbiztonsági oktatást kell biztosítani, lehetőleg az informatikai rendszer használata előtt, illetve az általuk használt informatikai infrastruktúra változásakor (pl. új hardver vagy szoftver használatba vétele előtt), valamint az információbiztonsági kockázatok jelentős változásakor, új kockázati elem megjelenésekor.

(3) Az oktatás előkészítése során az IBF feladata az alábbiak meghatározása:
a) a szükséges tanfolyamok (struktúra és témakör) meghatározása;
b) javaslat a képzésben részesítendő munkakörök/szerepkörök meghatározására;
c) oktatásra javasoltak meghatározása;
d) az oktatók személyére vonatkozó javaslattétel (amennyiben a képzés nem külső szervezésű).

(4) Az információbiztonsági tudatossági oktatáson való részvétel kötelező rendszeresen évente egy alkalommal, továbbá eseti jelleggel a következő események bekövetkezése után:
a) jelen Szabályzat hatályba lépését vagy jelentős módosulását követően, az új vagy módosított szabályzatok ismertetése érdekében;
b) új foglalkoztatott belépésekor az új belépő részére, új munkavállalók számára belépő képzés biztosítása érdekében;
c) biztonsági esemény bekövetkezését és kivizsgálását követően az érintettek részére, amennyiben az IBF indokoltnak látja a képzést.

(5) Az oktatás megvalósítási módját tekintve lehet tantermi, e-learning oktatás vagy ezek kombinációja is. Az oktatásnak tartalmaznia kell a kialakított Szabályzat előírásait is. Az oktatásokat a Belső képzési központnak kell megszerveznie. Az oktatásokon való részvételt hitelt érdemlően kell dokumentálni.

(6) A képzéshez kapcsolódóan – igény esetén – az informatikai igazgatóság támogatást nyújt.

Az informatikai biztonság megsértése, veszélyeztetése esetén alkalmazandó következmények

**31. §** (1) Az informatikai szolgáltatások igénybevétele során elkövetett szabálysértésekért, illetve jogsértésekért a szolgáltatást igénybe vevő munkajogi, polgári jogi és büntetőjogi felelősséggel felelhet, amennyiben nem a szabályzatokban foglaltak szerint járt el és ennek következményeként jogsértés következett be.

(2) A Szabályzat, a vonatkozó jogszabályok, belső szabályzatok be nem tartása, valamint az informatikai biztonság veszélyeztetése, megsértése esetén a felhasználóval szemben fegyelmi, kártérítési, szabálysértési, illetve büntetőjogi felelősségre vonásnak lehet helye a vonatkozó jogszabályok, szabályzatok, illetve a Kollektív Szerződésben meghatározottak szerint.

(3) Az Információbiztonsági szabályok megsértésének gyanúja, illetve ilyen szabálysértéssel kapcsolatos tisztázatlan körülmények felmerülése esetén, az előbbieket észlelő személynek, értesítenie és tájékoztatnia kell az IBF-et, aki indokoltság esetén javaslatot tehet az informatikai igazgató felé, vizsgálati eljárás lefolytatására. A javaslat alapján, az informatikai igazgató utasítást ad az eset kivizsgálására.

Informatikai eszközök azonosítása, nyilvántartása, vagyonleltár

**32. §** (1) Az Egyetem birtokában lévő informatikai vagyontárgyak egyértelmű azonosítása, nyilvántartása kötelező. Az ezekről felvett vagyonleltárt folyamatosan karban kell tartani. A kapcsolódó szabályokat a Pécsi Tudományegyetem Leltározási és Leltárkészítési szabályairól szóló kancellári utasítás tartalmazza, biztosítva ezzel a NIS2 követelményeinek való megfelelést

Fizikai biztonság
Az Egyetem létesítményeibe való bejutás

**33. §** (1) Az Egyetem területén működő elektronikus beléptető rendszerrel ellátott helyiségek és területek elektronikus beléptető kártyáinak igénylését és a használat rendjét a Pécsi Tudományegyetem Biztonsági Szabályzata tartalmazza.

(2) Az informatikai helyiségekbe való belépés rendjét az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály alakítja ki, működteti és szabályozza a jelen Szabályzatban foglalt előírásokra tekintettel.

Az informatikai helyiségek nyilvántartása

**34. §** (1) Informatikai helyiségek az Egyetem mindazon helyiségei, amelyekben az informatikai infrastruktúra központi elemei elhelyezésre kerülnek:

a) szerverek;
b) telefonközpontok;
c) hálózati elosztószekrények, központi hálózati eszközök;
d) alkalmazói és irodai szoftverek és informatikai rendszer- vagy eszköz dokumentációk törzspéldányai;
e) biztonsági mentések.

(3) Az informatikai helyiségek tételes nyilvántartásáról az Informatikai Igazgatóság tájékoztatása alapján az Egyetembiztonsági Osztály gondoskodik.

Informatikai helyiségek kialakításának alapvető szabályai

**35. §** (1) Az informatikai szolgáltatások fizikai komponensei (szerver, tároló alrendszer, router stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben informatikai helyiségekben működtethetők. A helyiségeket biztonságos mechanikus zárakkal (biztonsági zár, vagy beléptető kártyával működtethető zár) és beléptető rendszerrel kell ellátni.

(2) Az informatikai helyiségeket vagyonvédelmi célból lehetőség szerint kamerás megfigyelőrendszerrel szükséges ellátni és a vonatkozó jogszabályok szerint kell azokat üzemeltetni.

(3) Az informatikai helyiségekben a hatályos szabályozás szerinti tűzvédelmi minősítést el kell végezni, és a minősítéshez igazodó, oltás esetén a lehető legkisebb kárt okozó oltóberendezéssel kell rendelkezniük.

(4) Az informatikai helyiségek villám- és túlfeszültségvédelmét, valamint szünetmentes áramellátását biztosítani kell.

(5) A beléptető rendszer szükséges alapkonfigurációi: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépési kísérlet jelzése a biztonsági személyzet felé.

(6) Mind az informatikai helyiségek, mind a telephelyi egyéb helyiségek esetében a bejárati ajtónak zárt állapotban kell lennie, nyitvatartásuk csak a közlekedés idejére, felügyelet mellett engedélyezett.

(7) Az egyéb helyiségekben is gondoskodni kell a megfelelő tűz-, villám-, és túlfeszültség védelemről.

(8) Az informatikai helyiségekbe való belépési jogosultságot az Informatikai Igazgatóság igazgatója, vagy az informatikai üzemeltetésért felelős főosztályvezetője engedélyezheti, a helyiségek és a végezhető munka felsorolásával. A belépési jogosultsággal rendelkezők e jogosultságukat nem ruházhatják át másra.

(9) Amennyiben az informatikai helyiségekbe belépési jogosultsággal rendelkező egyetemi polgár jogosultságát átruházza vagy a jogosultságával egyéb módon visszaél, továbbá amennyiben az informatikai helyiségekbe belépési jogosultsággal nem rendelkező személy lép be, hallgató esetén fegyelmi, munkavállaló esetén munkáltatói felelősségre vonásnak van helye. Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli.

(10) Minden fenti helyiség esetén biztosítani kell azt a gépészeti hűtési kapacitást, ami a teljes termelt hőmennyiség biztonságos elvezetését automatikusan meg tudja oldani. Hasonló módon biztosítani kell azt az erősáramú ellátó kapacitást, ami a berendezések villamos energia ellátását túlterhelésmentesen el tudja látni. Az erősáramú ellátó rendszernek áramkör – szelektív túlterhelés védelemmel kell rendelkezniük. A megfogalmazottakon túl az erősáramú és gépészeti berendezéseknek redundánsnak kell lenniük, azaz egy meghibásodása nem okozhatja a helyiségben üzemelő eszközök leállását.

(11) Az informatikai helyiségekben minden olyan munkavégzés, ami az informatikai szolgáltatásokat vagy azok működését veszélyezteti, csak előzetes egyeztetés alapján, az Informatikai Igazgatóság munkatársa felügyelete mellett végezhető.

(12) Az egyeztetést, a munkálatokat végző szervezeti egység vagy cég és az Informatikai Igazgatóság üzemeltetésért felelős főosztályvezetője végzi.

(13) A helyiséget kiszolgáló gépészeti és erősáramú berendezések működését veszélyeztető munkák csak az Informatikai Igazgatóság üzemeltetésért felelős főosztályvezetője előzetes engedélyével folytathatók.

(14) A gépészeti, vagy erősáramú berendezéseken történő munkavégzésből eredő károkért és szolgáltatás kiesésért a munkát végző felel. Külső vállalkozó által végzett munkavégzés esetén a munkáért a munkák egyetemi megrendelője felel, kivétel, ha a szerződésben a felek másként rendelkeznek.

(15) Az informatikai helyiségeket kiszolgáló gépészeti és erősáramú rendszerekre külön karbantartási tervet kell készíteni, amelyet az Üzemeltetési és Beruházási Igazgatóság üzemeltetésért felelős vezetője állít össze és gondoskodik a végrehajtásáról. A tervet az Informatikai Igazgatóság üzemeltetésért felelős vezetői véleményezik és hagyják jóvá.

(16) A karbantartás során a felmerült biztonsági sérülékenységeket megfelelően kell kezelni, illetve úgy kell a karbantartásokat elvégezni, hogy újabb biztonsági kockázatok ne merüljenek fel. Ennek felelőse a karbantartást végrehajtó személy vagy szervezet.

(17) Az egyéb munkaterületek (pl. irodák) használatának módja megegyezik az általános egyetemi területek használati módjával.

(18) Privilegizált hozzáférést vagy kritikus adatokat tartalmazó kiegészítő rendszerkomponensek (mentési berendezés, fejlesztői rendszer, felügyelő terminál stb.) csak beléptető rendszerrel védett munkaszobában, irodában helyezhető el.

(19) Az informatikai célú helyiségekkel kapcsolatos kérdésekben, a ki- és átalakítás koordinációjáért, a szakmai biztonsági szempontok betartásáért az adott helyiséghez tartozó szervezeti egység vezetője és az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály vezetője a felelős.

(20) Az Egyetem területén kifejezetten informatikai szolgáltatások biztosítását lehetővé tévő, informatikai eszközöknek helyt adó informatikai helyiségekhez az informatikai igazgató által hitelesített, fényképes igazolvánnyal rendelkező munkavállaló férhet hozzá fizikailag, a helyiségben található eszközök

üzemeltetését kizárólag ezen személyek végezhetik. Egyéb személyek kizárólag ezen munkavállalók felügyelete mellett léphetnek és tartózkodhatnak ezekben a helyiségekben.

(21) Az informatikai helyiségekben üzembe állítandó új szolgáltatások, vagy nagyobb rendszerkonfiguráció módosítás esetén a telepítés előtt előzetesen konzultálni kell az erősáramú és hűtési igény biztosításáról a gépészeti és erősáramú rendszerek működéséért felelős vezetővel. A szükséges gépészeti és erősáramú módosításokat az új szolgáltatás üzembe állítása előtt el kell végezni.

(22) Az informatikai helyiségeken kívül húzódó kábeleket (telefon és gerinchálózati kábeleket) tartalmazó egyetemi, vagy szolgáltatói tulajdonú alépítmények, kábelaknák és védőcsövek kiemelten óvandó területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni, csak az Informatikai Igazgatóság üzemeltetéséért felelős vezetőinek előzetes engedélyével lehet.

Informatikai helyiségek kialakításának további szabályai

**36. §** (1) Az egyetemi informatikai infrastruktúra elhelyezésének és az egyes központi és tartalék informatikai helyiségek kiválasztásának és kialakításának során az egyes informatikai helyiségekben elhelyezésre kerülő informatikai eszközök üzemeltetési előírásaiban megfogalmazott környezeti paramétereknek megfelelő környezet kell biztosítani legalább az alábbi informatikai biztonsági szempontokat figyelembevételével:

a) a környezeti kockázatokat (füstérzékelő, vízbetörés érzékelő) folyamatosan figyelemmel kell kísérni. Az érzékelők karbantartását rendszeresen el kell végezni;
b) a hatályos tűzvédelmi előírások és szabályzatok szerint kell a tűzvédelmet biztosítani. Automatikus tűzoltó palackok elhelyezése kötelező;
c) az informatikai helyiségekben használni tervezett erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet, és annak szintjét figyelemmel kell kísérni;
d) az informatikai helyiségeket úgy kell kialakítani, vagy az épület átépítése során csak úgy szabad a változtatásokat jóváhagyni, hogy a csővezetékek (pl. víz, csatorna, kondenzvíz, tűzi víz) rongálódásból származó károkkal szemben védve legyenek. Ahol az áthelyezésük nem megoldható, ott kiegészítő kontrollokat kell alkalmazni (pl. vízérzékelő, csepptálca);
e) behatolás védelem;
f) elhelyezés bejárattól, közösségi tértől távolabb, mindenképpen olyan helyen, ahová csak a portaszolgálaton, beléptető kapun át lehet eljutni, lehetőség szerint további fizikai védősávokkal (zárt folyosó, recepció) védve.
g) elhelyezés oly módon, hogy maga az informatikai helyiség ne legyen feltűnő, frekventált helyen (pl. büfé, dohányzásra kijelölt folyosószakasz mellett);
h) elhelyezés oly módon, hogy a helyiségek helye és jelentősége ne legyen bárki számára nyilvánvaló;
i) Áramellátás és áramvédelem:
   - szűrt és teljes túlfeszültség-védelemmel ellátott elektromos hálózat;
   - szünetmentes ideiglenes tartalék áramforrás (UPS), amely minimum 30 percig, de legalább az aggregátor elindításáig, illetve amennyiben nincs aggregátor, akkor legalább a rendszer rendeltetésszerű leállításáig biztosítsa az áramellátást;
   - tartós tartalék áramforrás (pl.: diesel generátor), amennyiben nincs lehetőség tartalék áramforrás használatára, kialakítására, úgy a szünetmentes tápegységet kell úgy méretezni, hogy az üzleti területek által meghatározott rendelkezésre állást az informatikai eszközökön biztosítani tudja.

(2) Informatikai helyiséget az informatikai igazgató előzetes hozzájárulása és az IBF tájékoztatása nélkül kialakítani és üzemeltetni tilos.

Informatikai eszközök védelme

Informatikai eszközök elhelyezése és védelme

**37. §** (1) Az informatikai eszközöket úgy kell elhelyezni, illetve védeni, hogy kockázati besorolásuknak megfelelő mértékű legyen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége szerint.

(2) A védelmi intézkedések biztosítják, hogy a különböző környezeti hatás miatt keletkező meghibásodások, adatvesztések csökkenjenek. A védelmi intézkedések érdekében:

a) a berendezéseket úgy kell elhelyezni, hogy a kapcsolódó munkaterületekre a szükségtelen belépéseket minimalizáljuk;
b) az érzékeny adatokat tároló és feldolgozó eszközök és munkahelyek monitorjait úgy kell elhelyezni (amennyiben lehetősége van rá, betekintésvédő fóliát alkalmazni), hogy azok használata közben illetéktelenek ne láthassák a képernyőn megjelenő adatokat;
c) intézkedéseket kell bevezetni a lopás, tűz, robbanóanyagok, füst, víz (vagy a vízellátás meghibásodása), köd, rázkódás, vegyi behatások, a villamos energiaellátás zavarai, elektromágneses sugárzás által okozott kockázatok minimalizálására;
d) az adatfeldolgozó eszközök közvetlen közelében folytatott étkezést, folyadékfogyasztást vagy dohányzást tiltani kell;
e) a környezeti feltételeket állandóan figyelni kell az olyan helyzetek felismerése érdekében, amelyek az adatfeldolgozó eszközök működésére negatív hatással lehetnek;
f) az adatfeldolgozó eszközöknek helyet adó épületeket villámvédelemmel, az elektromos tápellátást és a kommunikációs vonalakat pedig villámvédelmi szűrővel kell ellátni;
g) be kell tartani a tűzvédelmi és egyéb előírásokat a Pécsi Tudományegyetem Tűzvédelmi Szabályzatában foglaltaknak megfelelően.

(3) Az informatikai eszközöket folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében a gyártó útmutatása alapján, előírásoknak megfelelően karban kell tartani, amelyért az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály felelős.

A kábelezés biztonsága

**38. §** (1) Az adatátvitelt biztosító, az információszolgáltatásokat támogató elektromos, energiaátviteli és távközlési kábelhálózatot védeni kell az illetéktelen hozzáféréstől és a károsodástól.

(2) Fentiek megvalósításáért, ideértve a zárható szekrények és helyiségek kulcsainak tárolásáért, nyilvántartásáért az informatikai igazgató és az Egyetembiztonsági Osztályvezető felel.

(3) Gondoskodni kell a berendezések megfelelő védelméről az áramszünet és egyéb elektromos rendellenesség esetén.

Tápáramellátás

**39. §** (1) Gondoskodni kell a berendezések megfelelő védelméről az áramszünet és egyéb elektromos rendellenesség esetében.

(2) A magas rendelkezésre állású kategóriába sorolt központi informatikai infrastruktúra folyamatos tápáramellátását:

a) szünetmentes áramforrás;
b) több utas betáplálás;
c) tartalék-áramforrás

alkalmazásával kell biztosítani.

Az informatikai eszközök karbantartása

**40. §** (1) Az informatikai infrastruktúra, illetve eszközök karbantartását a gyártói útmutatás alapján, előírásszerűen kell elvégezni a folyamatos rendelkezésre állás érdekében. Ennek megvalósításáért az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály felelős.

(2) A Klinikai Központban, valamint azon szervezeti egységek esetében, melyek nem rendelkeznek a Kancellária által delegált területi informatikai referenssel, a karbantartási feladatok végrehajtásáért az adott szervezeti egység vezetője felelős.

Vagyontárgyak – telephelyről való eltávolítás, elszállítás

**41. §** (1) Az informatikai igazgató előzetes engedélye nélkül nem vihetők ki az Egyetem területéről az informatikai eszközök, szoftverek, kivéve a személyes leltárban található eszközöket és az ezekre telepített szoftvereket.

(2) Az Egyetem területéről kivitt eszközök és adatok használata során bekövetkező károkért az a személy viseli a felelősséget, aki az eszközt az Egyetem területéről kivitte. Az Egyetem területén kívüli használat, munkavégzés során mindazon elvek és gyakorlat követendő, amelyek az Egyetem területén belüli használat esetén is irányadók.

(3) Az adattároló médiumok, az információ és más értékek fokozott fenyegetettségnek vannak kitéve szállítás közben, ezért alábbi kontrollok megfelelő alkalmazásával kell gondoskodni biztonságukról:

a) az érzékeny, bizalmas információk, adathordozók szállítása esetén egyéb speciális kontrollokat is alkalmazni kell, mint:
   - a szállítandó eszközöket megfelelő csomagolással kell ellátni a fizikai károsodások (mágneses behatások) megelőzése érdekében;
   - zárható tároló doboz, vagy hordtáska alkalmazása;
   - olyan csomagolás alkalmazása, mely felbontás után nem zárható vissza az eredeti formában, így az esetleges illetéktelen hozzáférés felderíthető;
   - kriptográfiai módszerrel történő titkosítás elektronikus adathordozó esetén;
   - mobileszközök szállítása kizárólag zárolt állapotban hajtható végre;
b) javítás céljából az érzékeny információk, adathordozók elszállítására a következő kontrollokat kell alkalmazni:
   - merevlemez (munkaállomás, nyomtató stb.) törlése, amennyiben ez lehetséges;
   - amennyiben a vagyontárgyat (pl. szervizelésre kijelölt nyomtató) az Egyetem bármely területéről harmadik fél szállít el, a vagyontárgyat átadó személynek meg kell bizonyosodni arról, hogy a szállítást végző személy (pl. fényképes igazolvány, megbízólevél, céges bélyegző megléte stb. segítségével) valóban az adott szerződéses partnerhez tartozik, illetve a vagyontárgyat hiánytalanul átvette-e (pl.: felkerül a teherautóra) – az átvételről átadás-átvételi nyilatkozat kiállítása szükséges.

A mobil informatikai eszközök biztonságos használata

**42. §** (1) A mobil eszköz használatát a szervezeti egység vezetője hagyja jóvá. Az Egyetem tulajdonában lévő mobil eszközök munkavégzés céljából kerülnek átadásra. A Mobil eszközök használatának eljárásrendje szabályozza.

(2) A mobil eszközök használatára vonatkozóan legalább az alábbi irányelvek betartása kötelező:

a) tilos felügyelet nélkül nyilvános helyen, gépkocsiban hagyni;
b) az Egyetem informatikai rendszeréhez kapcsolódni csak az Egyetem eszközével és az Informatikai Igazgatóság által biztosított módon (pl. VPN) lehet;
c) gyártó előírásokat mindig be kell tartani az eszköz védelme érdekében, ez biztosítja az eszközök hosszú távú működőképességét és biztonságát;
d) amennyiben az Egyetem informatikai rendszeréhez idegen tulajdonú eszköz csatlakoztatása szükséges, arra csak írásbeli engedély alapján kerülhet sor;
e) mobil eszköz elhagyása, elvesztése vagy másnak tartós használatra való átadásakor, amennyiben az eszközön be van állítva valamilyen egyetemi informatikai szolgáltatás elérése, a felhasználó köteles bejelentést tenni az Egyetem IT Ügyfélszolgálatának a szolgáltatás és az eszköz közti kapcsolat mielőbbi törlése érdekében.

Az informatikai eszközökön adatok biztonságos megsemmisítése, az eszközök újra felhasználása

**43. §** (1) A használatból kivont információ-feldolgozó eszközöket szükség esetén egy hónapig raktározni lehet az esetleges visszaállítás érdekében, feliratozva, illetéktelen hozzáféréstől védve, annak érdekében, hogy fontos információk ne semmisüljenek meg és ne szivárogjanak ki.

(2) Az adott szervezeti egység kezelésében lévő adathordozók tekintetében a megsemmisítését vagy újra felhasználását kizárólag az Adatgazda kezdeményezheti.

(3) Amennyiben a nagy mennyiségű adathordozók megsemmisítését harmadik fél végzi, a megsemmisítést kizárólag erre a feladatra megfelelő felkészültséggel rendelkező partner végezheti. Az adathordozók megsemmisítésére irányuló szerződésben kell külön rögzíteni a titoktartási feltételeket, illetve a szerződőnek garanciát kell vállalni az adatok visszaállíthatatlan megsemmisítésére, a teljes és időbeli korlátozás nélküli titoktartásra is.

(4) Az eszközökben található adathordozókról az adatokat újra felhasználás előtt visszaállíthatatlan módszerrel törölni (WIPE) kell, akkor is, ha az nem tartalmaz bizalmas adatokat.

(5) Az informatikai eszközök selejtezéséről A Pécsi Tudományegyetem felesleges vagyontárgyak selejtezéséről, belső hasznosításáról szóló szabályzata rendelkezik

## 5. fejezet Informatikai üzemeltetés, fejlesztés biztonsága, beszerzése

Általános rendelkezések

**44. §** (1) Az informatikai szolgáltatások beszerzésére, fejlesztésére vonatkozó igényt minden esetben az Egyetemi IT Ügyfélszolgálatán, e-mailen, vagy az önkiszolgáló ügyfélszolgálati rendszerben kell jelezni. A telefonon, illetve nem az ügyfélszolgálaton jelzett igény az írásos megkeresést megelőzően nem kezelhető.

(2) Új informatikai szolgáltatás bevezetését megelőzően az adott szolgáltatásért felelős szolgáltatásgazda vagy alkalmazásgazda kijelölése szükséges. Ennek a kijelölésnek szigorúan dokumentáltnak kell lennie, és rögzítésre kell kerülnie a Rendszerkatalógusban, amely a szolgáltatások, felelősségek és konfigurációk teljes átláthatóságát és biztonságát biztosítja.

(3) Az informatikai üzemeltetésre, fejlesztésre és beszerzésre vonatkozóan a Pécsi Tudományegyetem Informatikai Szabályzatában foglaltak az irányadók.

Dokumentált üzemeltetési eljárások

**45. §** (1) A magas szintű szolgáltatásnyújtás elengedhetetlen feltétele az informatikai infrastruktúra esetében a megfelelően dokumentált, egységes elvek szerint történő üzemeltetés, amit az Konfigurációkezelési eljárásrendben foglaltaknak megfelelően szükséges kialakítani. A kapcsolódó szabályozókat, munkautasításokat, üzemeltetési kézikönyveket minden informatikai szereplő számára elérhetővé kell tenni.

(2) Az informatikai szolgáltatásokkal összefüggő minden változást nyomon követhető módon dokumentálni szükséges, így különösen:

a) a hozzáférések engedélyezését, módosítását;
b) a rendszer konfigurációk módosítását;
c) a fizikai hozzáféréseket.

(3) Minden szolgáltatás esetében az adott szolgáltatásra szabottan szükséges a dokumentációs rendet kidolgozni.

Változáskezelés

**46. §** (1) Változás alatt kell érteni nem csak a rendszerfejlesztéseket, hanem a rendszerek komponenseinek, illetve biztonsági beállításainak lényeges és az elfogadott standardoktól, szabályoktól eltérő módosítását is. Az információ-feldolgozó eszközök és rendszerek változtatásait nyomon kell követni, a változásokat előzetesen meg kell tervezni. A változás tervezéséhez tartozik a tesztelés, a végrehajtás részletes lépéseinek meghatározása, és szükség esetén a visszaállítási folyamatok kidolgozása. Minden változtatást engedélyeztetni kell az informatikai igazgatóval, és információbiztonsági érintettség esetén az IBF-el, biztosítva, hogy a változás megfelel az információbiztonsági előírásoknak és nem veszélyezteti a rendszer integritását.

(2) Minden olyan információ feldolgozó eszközökben és rendszerekben (éles, fejlesztői és teszt környezetben egyaránt) bekövetkező változást, amely hatással van az információbiztonságra, szigorúan felügyelet alatt kell tartani. Ezen változásoknak dokumentáltnak kell lenniük, biztosítva a teljes nyomon követhetőséget és megfelelőséget az információbiztonsági szabványokkal.

(3) Minden tervezett változtatásról, amely hatással lehet az információbiztonságra, valamint új védelmi intézkedés bevezetése esetén tájékoztatást kell küldeni az IBF részére is.

Informatikai beszerzések és fejlesztések

**47. §** (1) Az Egyetem által üzemeltetett (fejlesztési-, tesztelési- és éles) környezeteket fizikailag és logikailag egymástól külön kell választani. Ez az elválasztás alapvető fontosságú az információbiztonság fenntartása érdekében. A felhasználók számára világosan és egyértelműen azonosíthatóvá kell tenni, hogy melyik környezetben dolgoznak, ezzel is csökkentve a véletlen adatkeveredés vagy információszivárgás kockázatát.

(2) Az egyes rendszerekkel szemben támasztott követelményekről a Pécsi Tudományegyetem Informatikai Szabályzata rendelkezik.

(3) A külső fejlesztésű rendszerek szerződésének kötelezően tartalmaznia kell a telepítési és használati feltételeket, valamint a fejlesztési lehetőségeket, verziókövetést. Ebben az esetben a fejlesztővel, szállítóval kötött szerződésben kell kitérni jelen Szabályzat 25. §-ában részletezett információbiztonsági követelményekre, melyet az IBF ellenőrizhet.

Hibakezelés, konfigurációkezelés

**48. §** A rendszerspecifikus követelmények részletesen meghatározzák az adott rendszerekre vonatkozó speciális biztonsági és működési feltételeket. Ezek a dokumentumok tartalmazzák az egyes rendszerek konfigurációjának kezelésére, valamint a hibák és rendellenességek kezelésére vonatkozó előírásokat, amelyek a rendszer integritásának, rendelkezésre állásának és bizalmasságának fenntartásához szükségesek. A rendszerspecifikus előírásoknak biztosítaniuk kell, hogy minden változtatás, karbantartási tevékenység, illetve hibajavítás szigorúan ellenőrzött és dokumentált módon történjen, összhangban az információbiztonsági követelményekkel és a szervezet által elfogadott biztonsági szabványokkal. Ezek az előírások magukban foglalják a hibák és incidensek kezelési folyamatainak részletezését, beleértve a hibajegyek létrehozását, nyomon követését, a hibák hatásainak értékelését, valamint a szükséges korrekciós és megelőző intézkedések végrehajtását, valamint a rendszerek konfigurációinak ellenőrzését és nyilvántartását, amely biztosítja, hogy a rendszerek állapotát bármikor vissza lehessen követni, és hogy minden változtatás megfelelően dokumentálva legyen. A konfigurációkezelés célja, hogy minimalizálja az információbiztonsági kockázatokat a rendszerekben bekövetkező változások esetén.

Tesztelés, a tesztadatok kezelése

**49. §** (1) Új rendszer fejlesztésének vagy meglévő módosításának megkezdésekor azonosítani kell a fejlesztéssel kapcsolatos kockázatokat, az Informatikai Alkalmazástámogatási és Fejlesztési Főosztályvezetője vagy az általa kijelölt személy felelőssége, hogy az érintett területeket bevonja a kockázatelemzésbe.

Amennyiben más (meglévő) rendszerhez is kapcsolódik, abban az esetben meg kell vizsgálni a kapcsolatot és az új sérülékenység felmerülése esetén, a kockázatelemzés frissítése szükséges.

(2) Az informatikai biztonsági kockázatok felmérése és az azokkal kapcsolatos javaslatok kidolgozása az IBF feladata. A kockázatok felmérése során figyelembe kell venni a rendszer fejlesztésének vagy módosításának minden aspektusát, beleértve a kapcsolódó rendszerek biztonságát és a lehetséges sérülékenységeket.

(3) Fejlesztési és tesztelési célokra valós (ügyfél) adatok csak akkor használhatók, ha azok előzetesen anonimizálásra, vagy álnevesítésre kerültek (synthetic/anonymised or pseudonymised database). Az éles adatok anonimizálása során olyan módszereket kell alkalmazni, amelyek biztosítják, hogy az adatokból a személyes vagy érzékeny információk ne legyenek visszanyerhetők. Az éles adatok álnevesítése során olyan módszereket kell alkalmazni, amelyek biztosítják, hogy személyes adatok és az érintett kapcsolatának helyreállítására kizárólag az arra jogosultsággal rendelkező adatgazda képes. Bármilyen, teszt- vagy fejlesztési rendszerbe átmásolt éles adat használatához előzetes jóváhagyás szükséges az adatgazda részéről. Az éles és a tesztrendszer jogosultsági beállításainak azonosnak kell lenniük annak érdekében, hogy a tesztelés során azonos körülmények között történjen az adatok kezelése. Ha a teszteléshez magasabb jogosultság szükséges, akkor csak anonimizált, vagy álnevesített adatok használata engedélyezett. A fejlesztői környezetben és a külső partnerek számára elérhető adatbázisban kizárólag anonimizált, vagy álnevesített adatok szerepelhetnek, hogy az érzékeny információkhoz való jogosulatlan hozzáférés megakadályozása érdekében.

(4) A tesztelési tervek és jegyzőkönyvek meglétét, valamint azok tartalmát az IBF bármikor ellenőrizheti. Az információbiztonsági ellenőrzések biztosítása érdekében az informatikai szolgáltató és a külső fejlesztők kötelesek hozzáférést biztosítani az IBF számára a kért dokumentumokhoz. Az ellenőrzések célja annak biztosítása, hogy a tesztelési folyamatok megfeleljenek az előírt biztonsági követelményeknek, és hogy a tesztelési környezetben használt adatok megfelelően védettek legyenek.

Kártékony kódok elleni védelem

Rosszindulatú szoftverek (malware) elleni védekezés

**50. §** (1) Az elektronikus információs rendszerek kilépési és belépési pontjain úgy kell kialakítani a kártékony kódok elleni védelmi eljárásokat, a kapcsolódó szabályozást és intézkedési tervet, hogy elsősorban felderítsék és megsemmisítsék azokat, továbbá:

a) lehetővé tegyék a folyamatos felügyelet ellátását;
b) a valós riasztások kiszűrését támogassák;
c) a súlyos gondatlanságot, esetleg szándékosságot jelentő esetek kiszűrését támogassák;
d) a kártékony kódok elleni védekezés általános helyzetének értékelését lehetővé tegyék;
e) az új fenyegetések időben történő felismerését biztosítsák.

(2) A vírusvédelmi rendszer információbiztonsági szempontból történő kiválasztása és jóváhagyása az IBF felelőssége. A kártékony kódok elleni védelemmel kapcsolatos üzemeltetési feladatokat, a konfigurációkezelési szabályokkal és eljárásokkal összhangban a vírusírtó rendszerhez és operációs rendszerekhez kapcsolódó frissítések kezelését az Informatikai Igazgatóság látja el.

(3) Felhasználói számítógépeket (PC, notebook) – legyen az egyetemi vagy saját tulajdonú, mellyel a foglalkoztatottak egyetemi belső hálózathoz, szolgáltatáshoz, vagy erőforráshoz csatlakoznak - az Informatikai Igazgatóság által központilag biztosított Központi Desktop Menedzsment rendszerbe bevonni szükséges, mellyel a felhasználói számítógépek frissítési, biztonsági állapotának felügyelete (operációs rendszer, szoftverek, vírusvédelem), valamint a bekövetkezett biztonsági események központi naplózása biztosított.

Vírusvédelmi eljárások és védelmi eszközök

**51. §** (1) Az Egyetem informatikai hálózatában a vírusvédelmi intézkedések többszintű biztonsági rendszerként kerülnek kialakításra és felügyeletre az Informatikai Igazgatóság által. A vírusvédelmi rendszer célja, hogy megakadályozza a rosszindulatú kódok terjedését, és biztosítsa a szervezet adatainak és

rendszereinek biztonságát. A központilag üzemeltetett rendszerek esetében a hálózatba történő fertőzött eszköz belépése esetén az érintett eszközt azonnal izolálni kell a hálózat többi részétől, és meg kell kezdeni az incidenskezelési eljárást. Ebben a folyamatban a felhasználók kötelesek együttműködni az Informatikai Igazgatóság munkatársaival, ideértve az eszközök elkülönítését és a szükséges intézkedések végrehajtását. Több munkaállomás egyidejű fertőzése esetén az Informatikai Igazgatóság jogosult a teljes érintett hálózati szegmens izolálására.

(2) Az egyetemi informatikai infrastruktúrán belül csak olyan egyetemi tulajdonú eszközök használhatók, amelyek központi felügyelet alá bevonásra kerültek, továbbá naprakész vírusvédelmi rendszerrel rendelkeznek. Elavult vagy nem frissíthető operációs rendszerrel rendelkező (pl. műszert vezérlő) eszközöket szeparált, zárt hálózatban kell üzemeltetni. Ezeket az eszközöket az internetre csatlakoztatni tilos, és csak szigorúan ellenőrzött körülmények között használhatók.

(3) A vírusvédelemre vonatkozó elemi szabályokat és előírásokat valamennyi felhasználó köteles szigorúan betartani. Amennyiben egy felhasználó bármilyen rosszindulatú szoftver, kártékony kód jelenlétére gyanakszik, akkor a gyanús eszköz vagy rendszer használatát haladéktalanul fel kell függesztenie, és az Egyetem IT Ügyfélszolgálatának jelezni kell.

(4) Minden felhasználónak kötelessége az adathordozókon kapott vagy letöltött fájlokat azonnal átvizsgálni a számítógépükre telepített vírusvédelmi szoftverrel. A vírusellenőrzési folyamatnak, ahol csak lehetséges, automatikusnak kell lennie, és a felhasználók számára előírt alapértelmezett beállításokkal kell működnie, hogy a manuális ellenőrzések elvégzése nélkül biztosítsa az állományok biztonságát.

(5) A vírusvédelmi rendszer frissítései központilag, felhasználói beavatkozás nélkül történnek. A vírusvédelmi ellenőrzések és frissítések időpontját lehetőség szerint úgy kell meghatározni, hogy azzal a felhasználókat ne akadályozzák a feladatuk elvégzésében. Az ellenőrzések eredményeit vírusvédelmi naplókban kell megőrizni és visszakereshetővé kell tenni. A központi felügyelet és frissítések biztosítása garantálja, hogy minden eszköz naprakész legyen. A frissítéseket és konfigurációkezelést folyamatosan monitorozni kell.

## Hozzáférés a rendszerekhez

### Jogosultságkezelés

**52. §** (1) A szükséges jogosultságok beállítása a legkisebb jogosultság elvén alapszik. A jogosultságbeállítás célja, hogy a felhasználói hozzáférés teljes életciklusában biztosítsa, hogy a felhasználó csak azokhoz az informatikai rendszerekhez, azokban tárolt adatokhoz, programokhoz és szolgáltatásokhoz férjen hozzá, mely a munkaköri feladatok ellátásához feltétlenül szükségesek. A jogosultságok kezelése a teljes felhasználói életciklus során történik, amely magában foglalja a jogosultságok létrehozását, karbantartását és visszavonását. A jogosultságok kezeléséért a közvetlen munkahelyi vezető felel, aki köteles biztosítani, hogy a felhasználó kizárólag azokhoz az erőforrásokhoz férjen hozzá, amelyek a munkaköréhez szükségesek. Hozzáférés védelmi és jogosultságkezelési eljárásrend tartalmazza részletesen.

(2) Az informatikai szolgáltatások esetében minden felhasználó, beleértve az üzemeltetőket, fejlesztőket és végfelhasználókat is, csak a munkaköri leírásában rögzített feladatok ellátásához szükséges, legszűkebb körű jogosultságokkal rendelkezhet. A rendszerekhez való hozzáférés csak megfelelő hitelesítéssel történhet, amely biztosítja, hogy illetéktelen személyek ne férjenek hozzá az informatikai erőforrásokhoz. Az azonosítás és hitelesítés folyamatát úgy kell kialakítani, hogy az biztonságos, nyomon követhető és auditálható legyen.

(3) Az Egyetem informatikai szolgáltatásainak igénybevételéhez szükséges jogosultságokat az Informatikai Igazgatóság felügyeli. Az informatikai szolgáltatásokhoz való hozzáférést a felhasználók megfelelő szakértelmének igazolásával (pl. vizsgáztatással) kell biztosítani. Minden hozzáférés igénylése dokumentált folyamaton keresztül történik, amely tartalmazza a szükséges képzések és minősítések követelményeit.

(4) A felhasználói jogosultságok rendszeres felülvizsgálata kötelező, és az adatgazdák felelősségi körébe tartozik. Az adatgazdák kötelesek biztosítani, hogy minden hozzáférési jogosultság naprakész legyen, és

kizárólag a szükséges erőforrásokhoz biztosítson hozzáférést. Az Informatikai Igazgatóság támogatja az adatgazdákat az adatszolgáltatással és a jogosultságok nyilvántartásának kezelésében.

(5) Az egyes informatikai szolgáltatásokhoz való hozzáférési jogköröket és jogosultsági szinteket az adatgazdáknak kell meghatározniuk a szolgáltatás kritikus fontosságát és a hozzáférési szintek biztonsági követelményeit figyelembe véve. Minden felhasználóhoz hozzárendelt jogosultságot dokumentálni kell, és rendszeres felülvizsgálat tárgyává kell tenni.

(6) Minden hozzáférési kísérletet, függetlenül annak szintjétől, hitelesíteni kell. Az azonosítási folyamatot, (pl.: a számítógépbe vagy alkalmazásokba való bejelentkezés), úgy kell kialakítani, hogy biztosított legyen a jogosultságok ellenőrzése és az illetéktelen hozzáférés megakadályozása.

(7) Az intézményi adatokhoz történő hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy a foglalkoztatottak csak a munkakörükkel kapcsolatos adatokat láthassák, illetve kezelhessék.

(8) Informatikai szolgáltatásokhoz módosítást és kritikus adatok lekérdezését lehetővé tevő hozzáférésre, kizárólag másik szolgáltatás vagy természetes személy lehet jogosult. Természetes személyek egy csoportja, közös használatú hozzáféréssel kizárólag mindenki számára hozzáférhető adatokhoz, vagy egy szervezeti egységen belül mindenki számára hozzáférhető adatokhoz történő hozzáféréshez (pl. egységen belüli közös hálózati meghajtó elérése közös használatú számítógépekről) rendelkezhet jogosultsággal.

(9) A jogosultságok nyilvántartását napra készen kell tartani és az adatgazda rendelkezése alapján, de minimum évente felül kell vizsgálni, és szükség esetén el kell végezni a módisításokat.

(10) Az informatikai szolgáltatások felhasználóinak azonosítása és a jogosultság kezelése központilag, erre a célra szolgáló központi címtárral kell megvalósítani azért, hogy a felhasználói adatbázis kezelése egységesen és konzisztensen valósuljon meg. Kivételt ez alól csak az informatikai igazgató engedélyével, indokolt esetben tehető. Lehetőség van továbbá szerződések alapján létrejött ún. föderációs azonosítási rendszerek (pl. eduID) használatára, azonban ilyen szolgáltatások esetében is az egyetemi felhasználók azonosítását a központi címtár alapján kell megoldani.

(11) A felhasználók egyedi azonosítását, jogosultságigénylés -és kezelés folyamatát dokumentálni kell a Pécsi Tudományegyetem Informatikai Szabályzatában, a kapcsolódó eljárásrendekben foglaltaknak megfelelően.
A munkavállalók esetében a Pécsi Tudományegyetem Informatikai Szabályzatának a Jogosultsági szintek meghatározása, hozzáférés szabályozása pontja tartalmazza a részletes leírást.

(12) Külső partnerek hozzáférését a 7/2017. kancellári utasítás a PTE informatikai rendszereihez a külső partnerek részére biztosított hozzáférések rendjéről szóló utasítás tartalmazza.

(13) A felhasználók kötelesek zárolni a munkaállomásukat, ha azt felügyelet nélkül hagyják, még rövid időre is, annak érdekében, hogy az illetéktelen hozzáférést megakadályozzák. Ez a biztonsági eljárás kulcsfontosságú a jogosulatlan hozzáférések elkerülése érdekében.

Jelszókezelés szabályai

**53. §** (1) Jelszavak használata az informatikai biztonság egyik meghatározó része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszavak fontosságával és a nem megfelelő jelszókezelés következményeivel. A felhasználói azonosítók és jelszavak átadásának bizalmasan kell történnie, és azokat csak biztonságos csatornákon keresztül szabad továbbítani.

(2) A felhasználók kötelessége a jelszavak megfelelő kezelése. A jelszó megváltoztatása kötelező az alábbi esetekben:

a) a felhasználói fiók létrehozása utáni első belépéskor;
b) az Informatikai Igazgatóság általi új jelszó beállítását követően;

c) amennyiben felmerül a gyanú, hogy a jelszó más személy tudomására jutott;
d) a jelszó érvényességi időtartamának lejártakor.

(3) A jelszavak bizalmas kezelésére vonatkozóan az alábbi irányelvek érvényesek:
a) a jelszót tilos másoknak bármilyen formában átadni, a jelszóról mások előtt beszélni;
b) a jelszót se a munkáltatói jogkör gyakorlóinak, közvetlen munkahelyi vezetőknek, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, még ha kifejezetten kérik ezt, akkor sem;
c) a felhasználónak tilos más felhasználó jelszavát megkérdeznie és tilos más felhasználó azonosítóját használnia annak belépése után, hasonlóképpen, a felhasználó nem engedheti meg más felhasználónak az azonosítója használatát.

(4) A jelszavak kiválasztása során az alábbi irányelveket kell betartani:
a) tilos a felhasználói nevet jelszóként használni;
b) a jelszót tilos titkosítatlan formában tárolni;
c) kerülni kell az egyszerű, egymást követő karakterekből álló jelszavakat, például azonos vagy egymást követő betűk vagy számok használatát;
d) nem javasolt a programok automatikus jelszó-megjegyző funkciójának alkalmazása;
e) javasolt olyan jelszavakat választani, melyek nehezen visszafejthetőek, de könnyen megjegyezhetőek, nem személyes adatokon alapulnak (pl. nem tartalmaz telefonszámot, gyermek nevét, születési dátumot, kedvenc háziállat nevét, cégnevet, rendszámot stb.) és nem szótári szó;
f) a felhasználói jelszavaknak minimálisan 12 karakter hosszúnak kell lenniük és tartalmazniuk kell minimum 3 karaktertípust az alábbiakból: nagybetűk, kisbetűk, számok;
g) Jelszóváltoztatáskor a felhasználó nem használhatja az előző 12 jelszavát.
h) Rendszergazdai, technikai, service account-ok minimum jelszó hossza 16 karakter.

(5) A jelszószabályok betartása minden felhasználónak jól felfogott saját érdeke. A felhasználó felelőssége, ha neki felróható mulasztása miatt a jelszava megismerése révén valaki visszaélést követ el.

(6) Hibás jelszóval történő bejelentkezési kísérletek maximális száma rendszerenként eltérő, de maximum 5 lehet. Ha a felhasználó túllépi a meghatározott kísérletszámot, a fiókot zárolni kell és erről az Egyetem IT Ügyfélszolgálata automatikusan értesítést kap. A fiók zárolása 6 óra elteltével automatikusan feloldódik.

A felhasználói jogosultságok felülvizsgálata

**54. §** (1) Az adatgazdáknak rendszeresen, de legalább évente egyszer kötelességük felülvizsgálni a felhasználói hozzáférési jogosultságokat annak érdekében, hogy a felhasználók csak a munkakörükhöz szükséges hozzáférésekkel rendelkezzenek. A felülvizsgálat során meg kell győződni arról, hogy a jogosultságok megfelelnek a legkisebb jogosultság elvének, és csak a szükséges erőforrásokhoz biztosítanak hozzáférést, melyet jegyzőkönyvben szükséges rögzíteni.

(2) A felhasználói jogosultságok változásait – legyen szó új jogosultságok kiadásáról, meglévő jogosultságok érvényesítéséről vagy visszavonásáról – dokumentálni kell. Minden ilyen változásnak nyomonkövethetőnek és auditálhatónak kell lennie. A jogosultságok módosítását és azok visszakereshetőségét biztosító nyilvántartási rendszer létrehozása, vezetése kötelező.

Távoli elérés

**55. §** (1) Az Egyetem által biztosított VPN rendszer célja a biztonságos távoli hozzáférés lehetőségének megteremtése az Egyetem dolgozói és harmadik felek számára, az egyetem telephelyein kívül végzett munka elvégzéséhez. A VPN rendszert kizárólag munkavégzési célokra és a felhasználók munkaköréhez kapcsolódó tevékenységek végzésére lehet használni. A távoli hozzáférés során biztosítani kell az adatok bizalmasságát, integritását és elérhetőségét. Távoli hozzáférés engedélyezési, használati eljárásrend szabályozza.

(2) A felhasználók az Egyetem hálózatához távolról kizárólag VPN alkalmazás használatával kapcsolódhatnak. A távoli elérés létesítése kiemelt információbiztonsági kockázatot jelent, melyre az ezt

biztosító jogok és az üzemeltetés teljes időszaka alatt figyelemmel kell lenni. A VPN segítségével csatlakoztatott eszközök fokozott védelme, karbantartása, vírusvédelme, az illetéktelen hozzáférés megakadályozása a felhasználó kötelessége.

(3) Az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály munkatársa felelős a VPN kapcsolatok megfelelő konfigurálásáért, beleértve a beállítások biztonságos megvalósítását. Az adott szervezeti egység vezetője felelős a VPN igénylés jóváhagyásáért, és gondoskodni arról, hogy a jogosultságok a legkisebb jogosultság elvén alapuljanak.

(4) A felhasználó köteles a távoli munkavégzésre előírt szabályokat teljeskörűen betartani. Ideértve a biztonsági előírásokat is. A távoli hozzáférés kockázatait kezelni kell, beleértve a megfelelő biztonsági intézkedések, (pl.: a tűzfalak és vírusvédelmi rendszerek) alkalmazását.

(5) A VPN kapcsolat kizárólag személyi tűzfal és vírusvédelmi szoftver aktív használata mellett engedélyezett. A távoli hozzáférést biztosító rendszereken megfelelő biztonsági intézkedéseket kell alkalmazni a külső támadások elleni védelem érdekében.

(6) A VPN hozzáférésre vonatkozó igényt a https://sm.pte.hu oldalon keresztül elérhető online formanyomtatvány kitöltésével kell benyújtani. A hozzáférési igényeket dokumentált eljárás keretében kell kezelni, és minden hozzáférés-engedélyezési folyamatnak auditálhatónak kell lennie.

Hálózat biztonság

**56. §** (1) Az egyetemi hálózat használata során minden felhasználó köteles betartani és magára nézve kötelezőnek elfogadni az érvényben lévő, hálózat használatára vonatkozó szabályokat, ideértve az Egyetem hálózatának szabályait (UPNET AUP). A hálózathoz való hozzáférés szigorú szabályok alapján történik, és a felhasználóknak biztosítaniuk kell a hálózat megfelelő használatát.

(2) Az internet-hozzáférés használatakor a felhasználónak be kell tartania az Egyetem internet-szolgáltatójának, a Kormányzati Informatikai Fejlesztési Ügynökség szabályzatát is. A külső kapcsolódások biztonságát minden esetben biztosítani kell a hálózati szabályok betartásával.

(3) Az egyetemi hálózathoz való hozzáférés csak megfelelő felhasználói azonosítással engedélyezett, amely biztosítja a jogosulatlan hozzáférések kizárását. Minden felhasználónak hitelesítési eljáráson kell keresztülmennie, mielőtt hozzáférést kap a hálózathoz.

(4) A felhasználók egyetemi hálózathoz való hozzáférését az adatbiztonsági követelmények biztosítása, valamint minőségbiztosítási okokból naplózni szükséges. A naplónak tartalmaznia kell a felhasználóhoz rendelt fizikai címeket, IP-címeket és felhasználóneveket.

(5) A naplózott adatokat 6 hónapig meg kell őrizni, majd meg kell semmisíteni.

(6) A további, szolgáltatás-specifikus naplózási intézkedéseket a szolgáltatás leírások tartalmazzák. A naplózási intézkedések során figyelembe kell venni az adatbiztonsági követelmények teljesítését.

(7) Személyes adatokat tartalmazó naplóbejegyzések rögzítése kizárólag legitim adatkezelési cél érdekében, megfelelő adatkezelési jogalappal, és a további adatvédelmi szabályok betartása mellett jogszerű. A személyes adatokat tartalmazó naplózás során az Informatikai Szabályzat 12-13. §-ait megfelelően alkalmazni kell.

(8) Személyes adatok, különösen betegadatok, hallgatói, tanulmányi adatok, bér és munkaügyi adatok, továbbá a gazdálkodási, valamint a kutatási adatok továbbítása informatikai hálózaton kizárólag megfelelő titkosítás mellett végezhető.

(9) Az informatikai szolgáltatások biztonságos távoli, nem egyetemi hálózatból történő elérését hitelesített, vég-vég titkosított VPN-en, vagy más titkosított, a két végpont között racionális időn belül vissza nem fejthető csatornán (pl. HTTPS) keresztül kell biztosítani.

(10) Egyetem informatikai rendszereinek biztonsága érdekében a hálózatot egymástól jól elkülöníthető logikai tartományokba kell osztani. Az egyes tartományok közti adatforgalmat tűzfal alkalmazásával szűrni kell, hogy megakadályozzák a jogosulatlan hozzáférést. A hálózatok menedzselését és felügyeletét az Informatikai Igazgatóság Infrastruktúra Szolgáltatási Főosztály Infrastruktúra Üzemeltetési Osztály Hálózat Üzemeltetési Csoportja lát el.

(11) A hálózati rendszereket védelemmel kell ellátni a túlterheléses (szolgáltatásmegtagadás jellegű) támadásokkal szemben, amelyek minimalizálják ezek hatásait, és biztosítják a rendszer rendelkezésre állását. A szolgáltatás megtagadásos támadások elleni védekezés kulcsfontosságú a rendszerek folyamatos működésének fenntartásához.

Biztonsági mentés, archiválás

**57. §** (1) Az Egyetem kezelésébenlévő, elektronikus formában tárolt információkról és adatokról rendszeres, meghatározott időközönként és indokolt esetben soron kívüli biztonsági mentéseket kell készíteni.

(2) Az informatikai rendszerekben kezeltadatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során már nem szükséges, azonban őrzésük indokolt, archiválni kell. Az adatok archiválása után gondoskodni kell azok őrzéséről az előírt őrzési időtartam végéig. Az őrzési idő lejártát követően az adatokat megfelelően biztonságosan törölni kell.

(3) A részletes biztonsági mentési, archiválási és visszatöltési rendszer leírását, az üzemeltetés kapcsán felmerülő feladatokat, illetve azok felelőseit a Pécsi Tudományegyetem mentésekre vonatkozó eljárásrendje(i) tartalmazza.

(4) Minden informatikai szolgáltatás az Informatikai Szabályzat 1. számú mellékletében meghatározott adatlapjának tartalmaznia kell az adott szolgáltatásra vonatkozó mentési és archiválási rendet (minimálisan meghatározva a mentendő adatok körét, a mentés módját és gyakoriságát, a mentések tárolási rendjét, megőrzési idejét és példányszámát, valamint a felülvizsgálat gyakoriságát).

(5) Az elvárásoknak megfelelő mentési módszerek technológiai kidolgozása az Informatikai Igazgatóság üzemeltetésért felelős vezetőjének a feladata. A mentési eljárásoknak biztosítaniuk kell az adatok megbízható és biztonságos mentését, valamint azok visszaállíthatóságát.

(6) A biztonsági mentési és archiválási rend betartásához szükséges erőforrások (hardver, szoftver, humán) biztosítása a Kancellár feladata.

(7) Az adatgazda kérése alapján az Informatikai Igazgatóság gondoskodik a telephelyen kívüli tárolású (offsite) biztonsági mentésekről.

(8) A biztonsági mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy a szolgáltatás működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén is helyreállítható legyen, illetve, hogy a kritikus rendszereknél a helyreállítási idő minimálisra csökkenjen, és az üzletmenet-folytonosság biztosított legyen.

(9) A szolgáltatások konfigurációs beállításait minden változás esetén, de minimum hetente kell menteni. A mentési eljárásnak lehetővé kell tennie egy adott állapot célirányos betöltését. A konfigurációs mentéseknek 10 előző állapotra, illetve minimum az előző 30 szolgáltatási napra ki kell terjedniük.

(10) A mentési eljárásnak lehetővé kell tennie az adatok tesztrendszerbe történő betöltését annak érdekében, hogy a mentések visszaállíthatósága rendszeresen ellenőrizhető legyen.

(11) Az adatok mentését minden esetben – lehetőség szerint éjszaka – úgy kell elvégezni, hogy az a lehető legkisebb módon befolyásolja az adott szolgáltatás használatát.

(12) Minden szolgáltatás esetében évente minimum egy alkalommal visszatöltési gyakorlatot, tesztet szükséges végezni, amely a mentések felhasználhatóságát ellenőrzi. A visszatöltési gyakorlat az éles szolgáltatással funkcionálisan egyező tesztrendszeren is teljesíthető. A gyakorlatoknak auditált és dokumentált folyamatok keretében kell történniük.

(13) A biztonsági mentések elkészítéséért, meglétéért és a visszatölthetőségéért az adott szolgáltatást üzemeltető személyzet a felelős.

(14) Új szolgáltatások bevezetésénél figyelembe kell venni a biztonsági mentéshez szükséges tárhelykapacitást.

(15) Amennyiben a technológia és a rendelkezésre álló erőforrások lehetővé teszik, úgy a mentéseket titkosítva szükséges tárolni.

Biztonsági mentések adathordozóinak kezelése

**58. §** (1) Az informatikai szolgáltatások adatállományainak biztonsági mentései intézményi és személyes adatokat tartalmazhatnak, ezért ezen adathordozók biztonságát biztosítani szükséges. Az adathordozókhoz való hozzáférés csak a megfelelő jogosultságokkal rendelkező személyek számára engedélyezett. Minden hozzáférést naplózni kell, és a naplózott adatokat rendszeresen felül kell vizsgálni annak érdekében, hogy biztosítsuk az illetéktelen hozzáférés kizárását.

(2) A biztonsági mentéseket tartalmazó adathordozók kizárólag zárható, tűzálló páncélszekrényben tárolhatóak. A páncélszekrényeknek minden esetben zárt állapotban kell lenniük, amikor nem történik adathordozó mozgatás. Az adathordozók tárolási helyén tűzálló és vízálló védelmet is biztosítani kell, hogy az esetleges katasztrófák (pl. tűz, árvíz) esetén az adatok ne sérüljenek. Az adathordozók tárolási helyének hozzáférését rendszeresen felül kell vizsgálni, hogy biztosítsák az adatok bizalmasságát és integritását.

(3) A biztonsági mentésre szolgáló adathordozókról nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell az adathordozó típusát, azonosítóját, a tárolási helyét, a mentések időpontját és a hozzáférésre jogosult személyek listáját. A nyilvántartást digitálisan is meg kell őrizni, hogy az auditálási és visszakeresési célokra mindig hozzáférhető legyen. A nyilvántartások rendszeres frissítését és azok integritását biztosítani kell, és a nyilvántartásokat legalább évente auditálni szükséges.

(4) A mentések adathordozóinak használatból történő kivonása után azokat meg kell semmisíteni. Az adathordozók megsemmisítését olyan módszerekkel kell végezni, amelyek biztosítják az adatok visszanyerhetetlenségét. Ilyen módszerek lehetnek a fizikai megsemmisítés (pl. zúzás, elégetés), vagy a digitális adathordozók esetében a visszafordíthatatlan adatmegsemmisítési módszerek (pl. adatfelülírás többszörös algoritmusokkal). A megsemmisítési folyamatot a felelős személyzetnek hitelesítenie kell, és az erről készült jegyzőkönyvet biztonságosan tárolni kell a jogi és auditcélok miatt.

(5) Az adathordozókat rendszeres fizikai és technológiai ellenőrzéseknek kell alávetni a hibák, sérülések vagy biztonsági problémák azonosítása érdekében.

(6) Az adathordozók titkosítása kötelező, ha azok érzékeny vagy bizalmas adatokat tartalmaznak. A titkosításnak biztosítania kell, hogy az adatok csak az arra jogosult személyek által olvashatók legyenek. A titkosítási eljárásokat rendszeresen felül kell vizsgálni, és az elérhető legmodernebb titkosítási technológiákat kell alkalmazni.

## Naplózás és monitoring

### Naplózás általános szabályai

**59. §** (1) A naplózási architektúrát úgy kell kialakítani, hogy a különböző rendszerek naplóállományainak egységes értelmezhetősége biztosított legyen. A naplózási architektúra kialakítása Infrastruktúra Szolgáltatási Főosztály vezetőjének felelőssége.

(2) A rendszergazdák felelnek az egyes rendszerekben a naplózási beállítások naprakészen tartásáért, biztosítva a naplózási események folyamatos, biztonságos rögzítését és tárolását. Minden naplózási tevékenységet rendszeresen felül kell vizsgálni a megfelelőség biztosítása érdekében.

(3) A naplóállományokhoz való hozzáférési jogosultságokat az informatikai igazgató hagyja jóvá, az IBF ellenőrzi, nyilvántartását az Informatikai Igazgatóság végzi. A naplóállományokhoz való hozzáférés szigorúan ellenőrzött, és csak a megfelelő jogosultságokkal rendelkező személyek férnek hozzá.

### Naplózandó események

**60. §** (1) Az Egyetem informatikai rendszerében automatikus naplót kell vezetnie az informatikai rendszer biztonsági szempontból lényeges tevékenységéről.

(2) A naplózásnak ki kell terjednie:
a) a jelen Szabályzatban meghatározott minden lényeges eseményekre, amely hatással lehet az információbiztonságra, és ezeket folyamatosan figyelni kell;
b) az arra felhatalmazással rendelkező személyek által meghatározott, ideiglenesen naplózandó eseményekre.

(3) Ideiglenes naplózást rendelhet el a naplózandó esemény, a naplózás időtartamának és céljának pontos megjelölésével, írásban:
a) az Adatgazda;
b) az informatikai igazgató;
c) az IBF;
d) a szakterületi vezető (igazgató, osztályvezető).

(4) A naplózandó események körét az informatikai igazgató és az információbiztonsági felelős együttesen határozza meg.

(5) A naplózandó események áttekintése része az Szabályzat rendszeres felülvizsgálatának. A naplózási rendszernek rugalmasnak kell lennie, hogy az újonnan felmerülő kockázatokra is reagálni tudjon.

(6) Az IBF meghatározott időközönként ellenőrzi, hogy az egyes rendszerek naplózási beállításai megfelelnek-e a naplózási események nyilvántartásának.

### Eseménynaplók tárolása

**61. §** (1) A naplóállományokhoz való hozzáférés ellenőrzött és dokumentált kell legyen, biztosítva az adatok bizalmasságát, integritását és rendelkezésre állását. A naplók tárolását úgy kell kialakítani, hogy azok hozzáférése, módosítása és megőrzése megfeleljen az Egyetem biztonsági irányelveinek. Bármilyen biztonsági esemény bekövetkezése esetén az eseménynaplók tartalmazzák azokat az információkat, melyek az utólagos vizsgálatok végrehajtásához szükségesek, ezért az eseménynaplók tárolásának minimum szabályai az alábbiak:
a) a naplóadatoknak sértetlenül rendelkezésre kell állniuk az elévülési időn belül;
b) az éles környezetben minimum a teljes mentések közötti időtartamnak megfelelő naplóállományokat kell tárolni;
c) biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani;

d) az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

(2) Biztonsági események, illetve incidensek kivizsgálása esetén az érintett rendszer (ügyviteli és technológiai egyaránt) üzemeltetőjének (legyen az az informatikai szolgáltató, a helyi üzemeltetés, vagy külső szállító) kötelessége átadni, betekintést biztosítani a kapcsolódó naplóállományokba a vizsgálatot koordináló IBF-nek.

(3) A naplózás során keletkező állományokat korlátozott hozzáféréssel, a bennük megjelenő adattartalom minősítése szerint kell kezelni, és a megjelenő adattartalom szerinti meghatározott ideig, központilag szükséges tárolni.

Rendszergazdák vagy más biztonsági szereplők által okozott biztonsági esemény kezelése

**62. §** A rendszergazda által okozott biztonsági esemény vagy annak gyanúja esetén az eszkalációs eljárás megegyezik az általános biztonsági esemény kezelési eljárással, azonban ilyen esetben tilos a rendszergazda tájékoztatása a vizsgálat lezárásáig. Az Informatikai Igazgatóság igazgatóját és az IBF-et haladéktalanul értesíteni szükséges. Minden biztonsági eseményt azonnal jelenteni kell, és biztosítani kell a titoktartást a vizsgálatok befejezéséig.

Monitorozás

**63. §** (1) Informatikai rendszerek esetében az alábbi esetekre szükséges azonnali riasztás beállítása:
a) szerverszoba fizikai biztonságának sérülése (illetéktelen behatolás, tűz, túlmelegedés, vízbeömlés stb.);
b) jogosulatlan hozzáférési kísérlet;
c) teljesítmény-problémák;
d) egyéb anomáliák és biztonsági események.

(2) A monitorozott eszközökről és felhasználókról az IT infrastruktúra monitorozó rendszer üzemeltetőjének naprakész nyilvántartással kell rendelkeznie, melybe kérésre betekintési lehetőséget kell biztosítania az IBF-nek az üzemeltető felügyelete mellett.

(3) A monitorozás során keletkező állományokat korlátozott hozzáféréssel, a bennük megjelenő adattartalom információbiztonsági osztályozása szerint kell kezelni, és a megjelenő adattartalom szerinti meghatározott ideig szükséges tárolni, illetve a keletkezett fájlok esetében a jelen fejezetben foglaltak szerint kell eljárni.

Órajelek szinkronizálása

**64. §** Az Egyetemen belül, illetve adott biztonsági tartományban működő valamennyi érintett információ-feldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz. A naplóbejegyzések időbélyegeinek előállításához ezt az órajelet kell használni.

Az informatikai szolgáltatások biztonsága

Elektronikus kommunikáció

**65. §** (1) A jelen Szabályzat az elektronikus kommunikáció alábbi, az Egyetemen belül elérhető eszközeire vonatkozóan tartalmaz előírásokat:
a) elektronikus levelezés;
b) internet;
c) webszolgáltatás;
d) PTE O365 szolgáltatás által biztosított kommunikációs csatornák.

(2) Ezen alkalmazások használata kizárólag a jogi követelményeknek megfelelően, az Egyetem előírásait és korlátozásait betartva, biztonsági, illetve hálózat menedzsment célú monitoring megvalósulása mellett megengedett az alábbiakban foglaltak szerint.

(3) Az elektronikus kommunikációra vonatkozó összes tevékenységet naplózni kell, és azokat az információbiztonsági előírásoknak megfelelően rendszeresen felül kell vizsgálni.

(4) A felhasználók kötelesek a titoktartási és adatvédelmi szabályok betartására az elektronikus kommunikáció során, és nem küldhetnek olyan adatokat, amelyek veszélyeztethetik az Egyetem információbiztonságát. A felhasználók figyelmét fel kell hívni az adathalász támadások és a nem biztonságos kommunikációs csatornák használatának kockázataira.

Elektronikus levelezés

**66. §** (1) Az elektronikus levelezési szolgáltatás célja az egyetemi tevékenységekkel összefüggő feladatok támogatása. Ennek értelmében az elektronikus levelezés kizárólag az oktatási, kutatási, társadalmi és munkaköri feladatok végzésére használható. Az elektronikus levelezés használatára vonatkozó jogosultságok csak az erre vonatkozó biztonsági szabályok megismerése után adható meg.

(2) Az elektronikus levelezésben lévő információkat védeni kell az alábbi módon:
a) biztosítani kell a pontos címzést és célba juttatást;
b) védeni kell az üzeneteket a jogosulatlan hozzáféréstől, módosítástól;
c) biztosítani kell a szolgáltatás megbízhatóságát és hozzáférhetőségét;
d) elektronikus aláírások használatát az arra feljogosítottaknak biztosítani kell;
e) azok a felhasználók használhatják az elektronikus levelezést, akik rendelkeznek az ehhez szükséges jogosultsággal.

Az elektronikus levelezés szabályai

**67. §** (1) Az e-mail címek lehetnek személyhez, szervezethez vagy egyéb csoporthoz (pl. projekt) rendelve. Minden esetben egyetemi- hallgatói azonosítóhoz kapcsolódnak.

(2) Egyetemi e-mail cím az egyetemi tevékenységgel összefüggésben használható, az alábbi alapvetésekre figyelemmel:
a) egyetemi polgárok a foglalkoztatásra irányuló jogviszonyukhoz, vagy hallgatói jogviszonyukhoz kapcsolódó ügyintézésre kizárólag egyetemi e-mail cím (az Informatikai Igazgatóság által biztosított központi e-mail cím, illetve postafiók) fogadható el;
b) minden egyetemi felhasználó egyedi e-mail címet kap, azt kizárólag a felhasználó maga veheti igénybe;
c) a felhasználó azonosítójának és jelszavának átadása más felhasználó részére tilos;
d) a munkahelyi e-mail címmel magánjellegű regisztrációt tenni különböző szabadon hozzáférhető, nem a munkavégzés céljával összeegyeztethető weboldalakon tilos;
e) a felhasználó elektronikus levelezésébe incidens megalapozott gyanúja esetén az IBF az informatikai igazgató engedélye alapján, a vonatkozó adatvédelmi és egyéb jogszabályi feltételek biztosítása mellett, betekintést nyerhet az informatikai és biztonsági szolgáltatókkal együttműködve;
f) az elektronikus üzenetek bizalmasságának, illetve hitelességének, letagadhatatlanságának védelme érdekében – az adatok biztonsági osztályba sorolásának megfelelően –aláírást (teljes név, beosztás és szervezeti egység) és titkosítást kell alkalmazni;
g) az egyetemi polgár köteles a jogviszonyával kapcsolatban tudomására jutott üzleti titkot megőrizni, ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely foglalkoztatásra irányuló jogviszonya, hallgatói jogviszonya betöltésével összefüggésben jutott a tudomására, és amelynek közlése az egyetemre vagy más személyre hátrányos következménnyel járhat;
h) az elektronikus levél mérete, a hozzá csatolható állománnyal együtt nem haladhatja meg a mindenkori szolgáltató által meghatározott korlátot, az ennél nagyobb levelek nem kerülnek elküldésre;
i) a felhasználók kötelesek rendszeresen frissíteni e-mail fiókjaik jelszavát, és biztosítani azok erősségét az Egyetem által meghatározott jelszópolitika szerint;
j) a felhasználóknak részt kell venniük az éves információbiztonsági képzésen és az azt követő teszten, amelynek célja az információbiztonsági tudatosság növelése;

k) a felhasználók kötelesek azonnal jelenteni az PTE IT Ügyfélszolgálatnak minden gyanús e-mailt, csatolmányt vagy linket, amelyet nem vártak, vagy amely biztonsági fenyegetést jelenthet. Ennek legegyszerűbb módja, az eredeti gyanús levél továbbítása az sd@pte.hu e-mail címre;
l) a hivatalos kommunikáció során az érintett felhasználók kötelesek aláírást (teljes név, beosztás és szervezeti egység) használni, különösen érzékeny vagy bizalmas információk továbbítása esetén;
m) a felhasználók nem tárolhatnak egyetemi e-mail fiókjukban olyan személyes adatokat vagy információkat, amelyek nem kapcsolódnak közvetlenül az egyetemi tevékenységükhöz;
n) a felhasználók kötelesek az e-mail fiókjaikhoz való hozzáférést megfelelően védeni, beleértve a kéttényezős hitelesítés alkalmazását, ha az elérhető.

(3) Az e-mailek küldésére vonatkozó főbb előírások az alábbiak:
a) a feladó köteles együttműködni az információbiztonsági kockázatok csökkentésében, ennek keretében különösen gondoskodnia kell annak ellenőrzéséről, hogy a címzettek jogosultak az emailben foglalt tartalom megismerésére, köteles továbbá a biztonsági eljárások betartására, a káros tartalmak elkerülésére és az adatvédelmi jogszabályoknak való megfelelésre;
b) más felhasználó nevében e-mailt küldeni tilos, kivéve a rendszerbeli meghatalmazási eljárás alkalmazásán keresztül (pl. asszisztens), továbbá a kifejezetten ilyen célra létrehozott alkalmazásokon és rendszereken, mint (pl.: hírlevélküldő);
c) a felhasználók kötelesek rendszeresen ellenőrizni e-mail fiókjaik tartalmát és törölni a szükségtelen vagy lejárt érvényességű üzeneteket, ezzel is csökkentve a biztonsági kockázatokat;
d) a rendszer a törölt elemeket meghatározott napig tárolja, utána véglegesen törlődnek a levelező rendszerből;
e) a leveleket mindig célzottan kell kiküldeni, a címzettek számosságára és megjelenítésére vonatkozó korlátozások figyelembevételével (a címzettek számát minimalizálni szükséges, csak a tárgyhoz köthető foglalkoztatottak részére címezzük, kivéve hírlevelek;
f) a címzettek listáját minden egyes küldés előtt gondosan ellenőrizni kell;
g) automatikus válaszüzenetek tartalmát minden esetben úgy kell meghatározni, hogy a benne megadott információkkal rosszindulatú fél ne tudjon visszaélni;
h) a felhasználók nem hozhatnak létre automatikus továbbítási szabályokat, amelyekkel a munkahelyi e-mail fiókjuk tartalmát külső címekre irányítják, kivéve, ha erre kifejezett engedélyt kaptak az Egyetemtől;
i) az Egyetem levelezőrendszerében tiltott a lánclevelezés, a kéretlen levelek (spam) tartalmak küldése. (A vizsgálat során biztosítani kell, hogy csak és kizárólag a biztonsági eseményhez kapcsolódó levelek kerüljenek vizsgálat alá);
j) az elektronikus levelezési rendszerbe beérkező leveleket minden esetben ellenőrizni kell, hogy nem tartalmaznak-e valamilyen, az Egyetem informatikai rendszerét veszélyeztető programot, kódrészletet, scriptet;
k) tilos a címinformáció hamisítása vagy a fejléc egyéb módon történő módosítása a feladó vagy a címzett személyazonosságának elrejtésére;
l) tilos vírusos levelek szándékos küldése;
m) tilos üzleti szempontból titkos, bizalmas, illetve belső információk jogosulatlan nyilvánosságra hozatala;
n) tilos minden ismeretlen kiterjesztésű e-mailhez csatolt állomány megnyitása;
o) tilos ismeretlen feladótól származó nem üzleti célú levelekben található csatolmány megnyitása;
p) tilos kéretlen levelek küldése, továbbítása;
q) tilos valótlan információt hordozó levelek tudatos továbbítása;
r) tilos az elküldött levél járulékos adatainak (pl. feladó e-mail címe, küldés időpontja) meghamisítása;
s) tilos privát postafiók tartalom automatikus továbbítása munkahelyi e-mail címre;
t) tilos az Egyetem elektronikus levelezési címjegyzékének kiadása harmadik fél számára.

(4) Az e-mailek fogadására vonatkozó főbb irányelvek az alábbiak:
a) Bizalmas információk továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről;
b) ismeretlen, gyanús feladótól érkezett csatolmányok, linkek megnyitása tilos. Kérdéses tartalmak megnyitása esetén a felhasználónak PTE IT Ügyfélszolgálatához kell fordulnia;

c) téves címzés miatt kapott e-mailt, annak felismerése után a felhasználónak haladéktalanul jeleznie kell a feladó- és a PTE Ügyfélszolgálata felé, és a levél tartalmának olvasása nélkül törölni kell. Az abban lévő tartalmak, információk, adatok jogtalan megismerése és kezelése tilos.
d) a felhasználók kötelesek minden kapott e-mail tartalmát hitelességi és biztonsági szempontból ellenőrizni, különösen, ha az ismeretlen feladótól származik.

(5) Az egyetemi elektronikus levelezési rendszeren keresztül küldött e-mailek naplózásra kerülnek biztonsági és audit célokra. A naplózott adatokhoz való hozzáférés szigorúan szabályozott, és csak az erre kijelölt biztonsági személyzet férhet hozzá a vizsgálatok során. A felhasználók kötelesek aktívan részt venni az Egyetem által szervezett biztonsági auditokban és ellenőrzésekben, és minden szükséges információt megadni az auditoroknak.

(6) A felhasználók kötelesek az e-mailek küldésekor és fogadásakor betartani a levélszűrésre és vírusvédelemre vonatkozó előírásokat, és együttműködni a PTE IT Ügyfélszolgálattal minden gyanús tevékenység jelentése és kezelése során.

Levélszűrés (spamkezelés)

**68. §** (1) Az elektronikus levelezés biztonságának megteremtését kéretlen levél (spam) szűrő rendszer alkalmazásával, valamint vírusvédelmi rendszer használatával kell biztosítani, melyet rendszeresen frissíteni kell.

(2) A levelek kéretlennek (spam) minősítését a kéretlen levélszűrő rendszer alkalmazásával kell elvégezni. A nem gyanús leveleket változatlanul továbbítani kell a címzett számára. A rendszer által spamnek minősülő levelet karanténba kell helyezni, a visszatartott levélről a címzettet tájékoztatni kell. A címzett a levelet a karanténban megtekintheti. A karanténban található kéretlen levelet a rendszernek a beérkezéstől számított egy hónap múlva automatikusan törölnie kell.

(3) Az egyetemi elektronikus levelezési rendszerben használt spam szűrő algoritmusokat folyamatosan fejleszteni és frissíteni kell, hogy a legújabb spam technikákat is hatékonyan kezeljék. A felhasználók részére rendszeres oktatásokat kell tartani a spam levelek felismeréséről és kezeléséről.

Hírlevelek kezelése

**69. §** (1) Az Egyetem infrastruktúráját használó hírlevelek kiküldésnek szabályait a Pécsi Tudományegyetem infrastruktúráját használó hírlevelek kiküldésnek szabályait az egyetem informatikai infrastruktúráján, az egyetemi levelezőrendszeren keresztül kiküldendő egyetemi hírlevelek kiküldésére vonatkozó rektori és kancellári együttes utasítás tartalmazza.

(2) A nem az Egyetem infrastruktúráját használó hírlevelekre való feliratkozás során a 2 § (2) pont szerinti rendelkezést kell követni. Egyetemi e-mail címet megadni hírlevélre való feliratkozáskor kizárólag a munkahelyi feladatokkal összefüggő esetekben szabad.

Internethasználat

**70. §** (1) A megbízható (egyetemi hálózat) és a nem megbízható (pl.: internet) hálózatokat csak az Egyetem tűzfalán keresztül lehet összekapcsolni. Az Egyetem rendszerében a felhasználóknak az internet használat során törekedni kell, hogy az ügyviteli folyamatok támogatására, illetve azokhoz kötődő információáramlásra használják.

(2) Az internet használata során az Egyetem fenntartja a jogot arra, hogy a felhasználók internet-forgalmát a személyes adatok védelmére vonatkozó szabályok betartásával naplózza, illetve ellenőrizze.

(3) Tiltott tevékenységek az internet használat során:
a) minden olyan tevékenység, ami a hatályos jogszabályokba ütközik, különös tekintettel az alábbiakra:
   − mások személyiségi jogainak megsértése;

- tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték);
- a szerzői jogok megsértése;
- szoftver szándékos és tudatos illegális terjesztése;

b) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység;
c) a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok, trójai programok, hacker eszközök, férgek);
d) hálózati forgalom lehallgatása, megfigyelése, kivéve, ha ez az adott munkakörhöz kapcsolódik;
e) Az internetről a legálisan hozzáférhető programok letöltése rendszergazdai jogosultsággal rendelkező felhasználó által lehetséges az információbiztonsági ellenőrzést követően;
f) a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, illetve biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
g) a felhasználói azonosítóval csak annak tulajdonosa jelentkezhet be. Az adatokhoz történő hozzáférés érdekében választott jelszó titkosságának megőrzése a felhasználó felelőssége. Egy adott azonosítóról folytatott tevékenységért mindig annak tulajdonosa felel, az azonosító kölcsönadása nem megengedett, így felelősségre vonás esetén ez az indok nem elfogadható;
h) minden felhasználó látogatására jogosult, ezért tilos továbbá:
   - sértő, társadalomra veszélyes, jó erkölcsbe ütköző szöveg, kép, ábra vagy egyéb formájú információ publikálása, letöltése;
   - az interneten elérhető szolgáltatást, bármilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt vagy díjszabást sértő módon használni;
   - bármelyik számítógép-hálózat biztonságát rombolni, illetve gyengíteni, más felhasználó jogosultságát jogosulatlanul használni;
   - bármilyen internetes végpontra, illetve hálózati eszközre jogosulatlanul csatlakozni, vagy ezzel próbálkozni;
   - bármely végpont működését megzavarni vagy azt az Egyetem hálózatáról, vagy annak igénybevételével szándékos túlterhelni (DOS támadás);
   - egyetemi tulajdonú eszközöket internetes számítógép erőforrás megosztásokhoz használni;
   - a hálózatot a szerzői jogvédelem alá eső anyagok átvitelére használni (még közvetetten is), ha az átvitel során mások szerzői joga sérül;
   - tilos kikapcsolni a munkaállomásra telepített biztonsági szoftvereket, eszközöket;
i) nem látogathatóak olyan oldalak, melyek megtekintése vagy használata a hivatalos egyetemi tevékenységgel össze nem egyeztethető:
   - az Egyetem érdekeit sértik;
   - rasszista tartalmúak;
   - erotikus oldalak;
   - kalóz oldalak;
   - terrorizmust támogató oldalak;
   - fegyverekre vonatkozó információkat tartalmaznak;
   - illegális kábítószerekre vonatkozó információkat tartalmaznak;
   - phishing (adathalász) oldalak;
   - internetes fogadási oldalak, szerencsejáték oldalak;
j) az Informatikai Igazgatóság informatikai üzemeltető személyzete által kialakított megoldásokon kívül tilos irodai munkaállomásokon külső frissítő szerverről való frissítés (pl. operációs rendszer-, vírusvédelmi rendszer-, alkalmazás-frissítések).

(4) A fentiekben meghatározott tiltott tevékenységeket végezni az Informatikai Igazgatóság előzetes engedélyével lehetséges, amennyiben oktatási-kutatási tevékenység ellátásához kapcsolódik.

Fájlkezelés/címtárkezelés

**71. §** (1) A fájlok kezelése során törekedni kell, hogy a tároló rendszerben az adott fájlnak minél kevesebb példánya tárolódjon.

(2) Nyilvános mappában tilos elhelyezni kritikus adatot tartalmazó dokumentumot.

(3) A felhasználóknak tilos megosztani az egyéni mappájukat, illetve a saját helyi tárolójuk bármely mappáját. Az olyan fájlok megosztása, amelyek nem az egyetemi folyamatokkal vannak összefüggésben, az egyetemi közös tárterületeken nem lehetséges.

(4) A szervezeti és az egyéni mappákban magánjellegű fájlok tárolása nem megengedett.

(5) A munkaállomás helyi adathordozóján tárolt adatok teljeskörűen nem kerülnek központilag mentésre. Részleges mentés a PTE O365 szolgáltatás keretében nyújtott OneDrive megoldással biztosított. A OneDrive-on kívül állományok mentéséről a felhasználónak kell gondoskodnia.

Webszolgáltatás

**72. §** (1) Az egyetemi központi honlapok (pl.) tartalmáért és módosításáért a Rektori Kabinet Kapcsolati Igazgatóság, karbantartásáért Informatikai Igazgatóság Informatikai Alkalmazástámogatási és Fejlesztési Főosztály felelős. A központi portálrendszerben lévő egyéb egyetemi szervezeti egységek honlapjainak tartalmáért és módosításáért az adott szervezeti egységek vezetői, karbantartásáért Informatikai Igazgatóság Alkalmazástámogatási és Fejlesztési Főosztály felelős. Az egyéb nem központi üzemeltetésű honlapok tartalmáért, módosításáért, kezeléséért és karbantartásáért a létrehozó szervezeti egység vezetője a felelős. A honlapokon kizárólag nyilvános, közérdekű információ jeleníthető meg.

(2) Az egyes egyetemi szervezetekre vonatkozó információkért az adott szervezet a felelős.

(3) Az Informatikai Igazgatóság felel a portál elérhetőségéért, az informatikai szolgáltatások rendelkezésre állásáért. A portál speciális információinak naprakészen tartása az adott terület tartalomfelelősének a feladata. A honlap igénylésével kapcsolatos előírások az Informatikai Igazgatóság honlapján találhatók.

PTE O365 szolgáltatás által biztosított kommunikációs csatornák

**73. §** Az Egyetemen a PTE O365 szolgáltatás keretében elérhető kommunikációs csatornák (pl. Teams, melyen keresztül csevegőszolgáltatás és videókonferencia is elérhető további beépített szolgáltatások mellett) használatára az e-mailekre vonatkozó általános alapelvek az érvényesek.

Kriptográfiai eszközök használata

**74. §** Az Egyetem az általa kezelt bizalmas és annál magasabb biztonsági besorolású adatok tárolása és továbbítása során kriptográfiai eszközöket alkalmaz annak érdekben, hogy csökkentse az érintett adatok sérülésének kockázatát és megőrizze azok bizalmasságát.

Titkosítás

**75. §** (1) A titkosítás alkalmazása nem kötelező a kizárólag közérdekű és a közérdekből nyilvános adatok esetében. Bizalmas, illetve titkos adatok továbbítása informatikai hálózaton kizárólag megfelelő titkosítás mellett végezhető. Amennyiben a titkosítás aránytalanul nagy teherrel járna vagy lehetetlen, abban az esetben kockázatcsökkentő intézkedésekről kell gondoskodni.

(2) A titkosítás végrehajtásáért a rendszert üzemeltető vagy adatot tartalmazó eszköz esetében az adatgazda vagy az adatot szállító személy felel.

Elektronikus aláírás

**76. §** A hatályos jogszabályoknak megfelelő esetekben elektronikus aláírás is alkalmazható. Ezeket az adott rendszerek dokumentációi határozzák meg.

Hitelesítés

**77. §** Az elektronikus aláírással kapcsolatban csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatják el az elektronikus információs rendszerek az érintett szervezeten kívüli felhasználók hitelesítéséhez.

## 6. fejezet Záró és hatályba lépő rendelkezések

**78. §** Jelen Szabályzat a 2025. január 1. napján lép hatályba. Jelen Szabályzat hatályba lépésével egyidejűleg hatályát veszíti a Pécsi Tudományegyetem 2022. július 1. napján hatályba lépett Informatikai Biztonsági Szabályzata.

**79. §** (1) Jelen Szabályzat a kapcsolódó szabályzatokkal, utasításokkal együtt érvényes. A jelen Szabályzatban nem szabályozott kérdésekben a mindenkor hatályos jogszabályokat, illetve belső rendelkezéseket kell érvényesíteni.

Pécs. 2024. december 12.

| | |
|---|---|
| Dr. Miseta Attila s.k.<br>rektor | Decsi István s.k.<br>kancellár |

**Záradék:**
Jelen szabályzatot a Szenátus 214/2024. (12.12.) számú elektronikus úton hozott határozatával fogadta el.

Mellékletek

1. számú melléklet – Fogalomtár

2. számú melléklet – Kapcsolódó jogszabályok, szabályozások listája

3. számú melléklet – Információbiztonsági Politika

4. számú melléklet – Elektronikus információs rendszerek biztonsági osztályba sorolása

5. számú melléklet – Szervezetek biztonsági szintbe sorolása

6. számú melléklet – Adatosztályozó lap

7. számú melléklet - Eljárásrendek

**PTE Informatikai Biztonsági Szabályzat 1. számú melléklet**

Fogalomtár

**Adat:** az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

**Adatállomány:** az egy nyilvántartásban kezelt adatok összessége.

**Adatbiztonság:** az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

**Adatbiztonság megsértése:** az a cselekmény vagy mulasztás, amely ellentétben áll az adat védelmére vonatkozó biztonsági szabályokkal és amelynek következményei az adatot veszélyeztetik.

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

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

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

**Adathordozó:** az adat tárolására és terjesztésére alkalmas eszköz.

**Adatkezelés:** a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

**Adatkezelő:** az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

A**datgazda:** az Informatikai Szabályzatban meghatározott adatgazda

**Adatvédelem:** az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.

**Adminisztratív védelem:** szervezési és szabályozási úton megvalósított védelem.

**Auditálás:** előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.

**Backup rendszer:** az informatikai biztonság megvalósítása során az adatok rendelkezésre állását lehetővé tevő rendszer és programmásolatokat őrző rendszer.

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

**Bizalmasság:** Az Ibtv. szerint a bizalmasság 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.

**Biztonság:** olyan szervezeti állapot, melyben az Egyetemnek a lehető legkisebb veszélyekkel kell számolnia, szolgáltatásait a vállalt és előírt feltételekkel és korlátozások nélkül képes nyújtani, a feladatait, funkcióinak ellátását illetően érdemi hatást gyakorló veszteség nem éri, a lehetséges fenyegetettségek bekövetkezési valószínűségéből és a lehetséges kárértékekből származtatott kockázat a szervezet számára elfogadhatóan alacsony és a kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elviselhető tartományban marad. A védeni kívánt informatikai rendszer olyan, az Egyetem számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

**Biztonsági szint:** a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

**Biztonsági követelmények:** a kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.

**Biztonsági esemény:** az Ibtv. szerint a 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.

**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.

**Biztonsági esemény bejelentő csatorna:** A biztonsági esemény bejelentésére szolgáló elektronikus levélcím, amelyen a biztonsági eseményt észlelőnek haladéktalanul jelenteni kell a biztonsági eseményt. A biztonsági esemény bejelentő csatorna az Egyetemen az Informatikai Igazgatóság által a honlapján közzétett elektronikus cím, jelenleg: sd@pte.hu.

**Biztonsági osztályba sorolás:** az Ibtv. szerint a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.

**Biztonsági rendszer:** a biztonsági rendszer az információbiztonsági rendszerek összessége (logikai védelmet valósít meg, pl.: tűzfal, vírusvédelmi rendszer, jogosultág-nyilvántartó rendszer stb.).

**Biztonsági szintbe sorolás:** az Ibtv. szerint a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

**Biztonságos törlés:** olyan eljárás, ahol a törlést végző munkatárs nemcsak törli, hanem a számítógépén lévő Lomtárból, levelező rendszer esetén a Törölt elemek könyvtárból is törli az adatállományokat. A biztonsági törlés egy fajtája a visszaállíthatatlan törlés, amit minden esetben csak megfelelő szoftver, hardver, vagy fizikai megsemmisítő által az informatikai szolgáltató végezhet.

**Egyenszilárdság:** a biztonság és a biztonsági szabályzat az intézmény egészét, annak valamennyi tevékenységét teljesen átfogja, és annak minden pontján azonos erősségű.

**Elektronikus aláírás (digitális aláírás):** az informatikai rendszerben kezelt adathoz rendelt, kódolással előállított olyan jelsorozat, amely az adat hitelességének és sértetlenségének, valamint letagadhatatlanságának bizonyítására használható.

**Elektronikus információs rendszer:** az Ibtv. szerint a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

**Elektronikus információs rendszer biztonsága:** az Ibtv. szerint az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

**Elszámoltathatóság:** azon követelmény, amely meghatározza minden, az információval vagy az informatikai rendszerrel kapcsolatos tevékenység egyértelmű azonosíthatóságát, utólagos visszakövethetőségét és az adott tevékenységet végrehajtó személyt.

**Életciklus:** az elektronikusinformációsrendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam.

**Érintett:** bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül, vagy közvetve – azonosítható természetes személy.

**ETR**: a Neptun rendszer bevezetését megelőzőn alkalmazott, a tanulmányi és oktatási adminisztrációt támogató rendszer. Ennek keretében ún. EHA (egységes felhasználói azonosító) kódok kerültek kiadásra, melyek bizonyos egyetemi rendszerekben jelenleg is használatban vannak. Az EHA kód felépítése 7 (hét) betű és .PTE végződés.

**Felhasználó:** az a személy/rendszer, szervezet vagy csoport, aki (amely) az Egyetem által biztosított rendszerekhez erőforrásokhoz csatlakozik és/vagy az Egyetem által biztosított eszközt használ, valamint ennek során egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.

**Felhasználói azonosító:** az egyetemi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat, amely általában a felhasználó nevéből képződik.

**Felhasználói hitelesítés:** a felhasználó hitelességének ellenőrzése (a belépéskor minden felhasználó ellenőrzése) és különböző azonosító eszközök (pl.: jelszó, chip-kártya, biometrikus azonosítás stb.) alkalmazása.

**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 kizárólag 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.

**Fizikai védelem:** a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

**Folyamatosság:** az üzleti, egyetemi tevékenységek zavarmentes rendelkezésre állása. Folytonos védelem: olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

**Hálózat:** számítógépek (vagy általánosabban informatikai rendszerek) összekapcsolása és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége.

**Határvédelmi felelős:** az Infrastruktúra Szolgáltatási Főosztály keretében kijelölt felelős, amely az informatikai határvédelmi és határbiztonsági rendszerek felelőse. (Pl. tűzfalrendszerek, hálózati hozzáférés-védelem, behatolásérzékelő és -megelőző rendszerek, távoli biztonságos elérés, hálózat szegmentációja).

**Hitelesség:** az adat/információ (és az adathordozó) tulajdonsága, amellyel igazolhatjuk, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

**Hozzáférés:** olyan eljárás, amely valamely informatikai rendszer használója számára – jogosultságának függvényében – meghatározott célra, helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat.

**Hozzáférési jogosultság:** az informatikai rendszerben elvégezhető tevékenységekre vonatkozó engedély a felhasználó számára.

**Illegális szoftver:** az a szerzői jog védelme alatt álló szoftvertermék, amelynek a legalitás igazolásához szükséges dokumentumok (pl. licenc, számla, szállítólevél) nem mindegyike áll rendelkezésre, valamint a szoftver használata nem felel meg a licenc szerződés előírásainak.

**Illetéktelen személy:** olyan személy, aki az adat megismerésére nem jogosult.

**Incidens:** minden olyan informatikai vonatkozású esemény, ami nem része a normál működésnek és a felhasználókat akadályozza feladataik ellátásában. A szolgáltatási hiba típusú incidensek a szolgáltatási szintek csökkenésével járnak (vagy ezzel fenyegetnek), míg a szolgáltatási igény típusú incidensek általában valamilyen eszköz vagy információ biztosítását, módosítások végrehajtását igénylik. Egy incidensnek lezárásáig többféle állapota lehet.

**Információbiztonság:** az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság szavatolása.

**Informatikai biztonság:** az Egyetem informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

**Információbiztonsági dokumentációs rendszer:** többszintű, egymásra épülő rendszer, amely magába foglalja a biztonságpolitikai elvektől a szabályzatokon keresztül a munkautasítások szintjéig az információbiztonsági irányelveket, teendőket, szereplőket, azok feladatait, jogait, kötelességeit és felelősségeit.

**Informatikai rendszer:** információs-, ügyviteli-, egyetemi folyamat vagy szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége. A hardver-, szoftver-, kommunikációs eszközök és ezek kezelő / kiszolgáló szervezeteinek olyan együttese, amelyet az Egyetem működésével összhangban céljai megvalósítására használ.

**Információ-feldolgozó eszköz:** minden olyan számítástechnikai, telekommunikációs és egyéb kategóriájú elektronikai eszköz, mely képes a betáplált (input) adatokat manipulálni és a folyamat végén eredményeket, kimenő adatokat (output) produkálni – az azt használó személy számára értelmezhető formában.

**Információs vagyon:** adatok, információk, szellemi, erkölcsi javak összessége.

**Információbiztonsági Felelős:** az Ibtv. szerinti az elektronikus információs rendszer biztonságáért felelős személy, aki kinevezés útján látja el az információbiztonsági felelősi feladatokat; szakterületén ellenőríz, tanácsot ad, véleményez. Az Egyetemen a Pécsi Tudományegyetem igazgatásának szervezetére vonatkozó szabályzata (PTE SZMSZ 32. számú melléklet) 41/D. §-ban meghatározott feladatokat látja el. Egyik legfontosabb feladata, hogy a teljes egyetemi szervezeten belül kialakítsa és ellenőrizze azokat az információbiztonsági szabályokat, amelyek az informatikai rendszerekkel kapcsolatba lépőkre vonatkoznak.

**Információvédelem:** az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.

**Internet:** a világháló.

**Intranet:** az intézményen belüli Hálózat és annak szolgáltatásai.

**ITIL (IT Infrastructure Library):** az 1980-as években, Angliában több, információtechnológiával (IT) foglalkozó cég által a brit kormány támogatásával létrehozott dokumentumsorozat, amiben az üzleti folyamatok IT eszközökkel megvalósított támogatására a gyakorlatban alkalmazott, jól bevált, gyártótól független üzemeltetési ajánlásokat gyűjtötték össze. Jelen szabályzat hatálybalépésekor a harmadik verziónál tart, 5 fő kötetből, és az ezekhez kapcsolódó kiegészítő anyagokból áll. Az ITIL a leginkább használt megközelítés az IT szolgáltatás-menedzsmentre, és főképp Európában az üzemeltetés de facto szabványa. Kizárólag az informatika üzemeltetési és üzemeltetés-szervezési kérdéseivel foglalkozik, dokumentált, kidolgozott oktatási és vizsgarendszere van.

**Jogtiszta szoftver:** olyan számítógépes program – alkalmazás – amelynek használatára a felhasználó (pl.: jellemzően késztermék vételi vagy szoftver-fejlesztési vállalkozási szerződésbe foglalt licenc megállapodással) megszerezte a jogosultságot.

**Jogosultság:** a lehetőség megadása az informatikai rendszerben végzendő tevékenységek végrehajtására.

**Katasztrófa:** az informatikai rendszer folyamatos és rendeltetésszerű működésének megszakadása.

**Katasztrófahelyzet elhárítás tervezés:** az informatikai rendszer rendelkezésre állásának megszűnése, nagy mértékű csökkenése utáni visszaállításra vonatkozó tervezés (DRP – Disaster Recovery Planning).

**Kiberbiztonság:** a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez működtetéséhez.

**Kockázat:** az informatikai fenyegetettség mértéke, amely valamely fenyegető tényezőből ered és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze. Az Ibtv. szerint a kockázat a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

**Kockázatelemzés:** olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési valószínűségét és gyakoriságát. Az Ibtv. szerint a kockázatelemzés az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak),

fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

**Kockázatkezelés:** védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak. Az Ibtv. szerint az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

**Kockázatarányos védelem:** az a védelem, mely a kockázatokat a releváns fenyegetettségek bekövetkezési valószínűsége és a fenyegetettség bekövetkezésekor keletkező kár függvényeként kezeli, és ahol a védelemre fordított erőforrások értéke arányos a védendő értékek nagyságával, illetve kockázatcsökkentő képességével. Az Ibtv. szerint sz elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

**Kontrollok-óvintézkedések:** mindazok a fizikai-, adminisztratív-, technikai-, technológiai módok, eljárások, amelyeket védelmi célból tettek meg és a kockázatot csökkentik.

**Kriptográfia:** mindazoknak a matematikai eljárásoknak, algoritmusoknak és biztonsági rendszabályoknak a kutatása és alkalmazása, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.

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

**Külső közreműködő (harmadik fél):** olyan külső szervezet, hatóság, szerződéses partner (jogi vagy természetes személy), akinek tevékenysége indokolttá teszi az Egyetem belső használatú és annál magasabb minősítésű adataihoz vagy bármely informatikai rendszeréhez történő hozzáférést.

**Legális szoftver:** az a szerzői jog védelme alatt álló szoftvertermék, amelynek legalitásának igazolásához minden szükséges dokumentum (pl. licenc, számla, szállítólevél, ajándékozási szerződés) rendelkezésre áll, valamint a használata a szoftver licenc szerződés előírásainak megfelelő módon történik.

**Letagadhatatlanság:** a letagadhatatlanság azon követelmény, amely meghatározza, hogy a felhasználók egy későbbi időpontban ne tudják valamilyen okból önkényesen megtagadni az előzőekben általuk végrehajtott tranzakciót.

**Maradványkockázat:** az a tudatosan felvállalt kockázat, amely alapvetően – kis mértékben – annak ellenére is fennmarad, hogy a fenyegető tényezők ellen intézkedések eredményesen végrehajtásra kerültek.

**Megbízható működés:** az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.

**Mentés:** informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.

**Mentési médium:** adathordozó (a legtöbbször mágneses elven működő szalagos egység), amelyen a mentések által duplikált adattartalmat tárolják.

**Mobil eszköz:** Minden olyan számítástechnikai eszköz, amely fizikailag szabadon mozgatható és funkcionalitását betölti mozgás közben is. Ide sorolhatók a hordozható számítógépek, illetve a velük azonos adattárolási, adatkezelési és adatmegjelenítési funkciókkal bíró telekommunikációs eszközök (pl. tablet, notebook, okostelefon stb.), valamint a hordozható adattárolók (pl. külső merevlemez, pendrive stb.).

**Mobil kód:** olyan szoftver vagy kód, mely általában egy távoli számítógépről, hálózaton keresztül letöltve, határozott telepítési vagy indítási procedúra nélkül fut vagy futtatható a kliens gépen. Ilyenek például a scriptek (JavaScript, VBScript), Flash animációk, Java kisalkalmazások, MS Office dokumentumok makrói, ActiveX vezérlők.

**NEPTUN kód:** a NEPTUN rendszerszolgáltatásaihoz hozzáférést biztosító betűkből és számokból álló, legalább 6 karakter hosszúságú kód.

**Rendelkezésre állás:** az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai állandóan, illetve egy meghatározott időben hozzáférhetők és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Az Ibtv. szerint annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

**Sértetlenség:** az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, ép, módosulatlan. Informatikai rendszer tulajdonság, amely adott, ha a rendszerben kezelt adatokat, illetve az adatkezelést megvalósító összes többi rendszer komponenst csak az arra jogosultak és csak dokumentáltan változtatják meg, emellett minden egyéb (véletlen vagy szándékos) módosulás kizárt — vagyis az adatok és feldolgozási folyamataik pontosak és teljesek. Az Ibtv. szerint a 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.

**Személyes adat:** azonosított vagy azonosítható természetes személyre (továbbiakban: érintett) vonatkozó bármely információ, amely alapján az érintett 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. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

**Szolgáltatás- vagy alkalmazásgazda:** azon természetes személy (foglalkoztatott), aki az adott szolgáltatás vagy alkalmazás üzemeltetéséért felelős.

**Teljes körű védelem:** teljes körűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.

**Üzleti titok:** a működéshez, az üzletmenethez és a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.

**Üzletmenet folytonosság tervezés:** az egyetemi folyamatok rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek.

**Védelmi intézkedés:** a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési- vagy technikai eszközökkel tett intézkedés.

**Tűzfal:** A tűzfal (angolul firewall) célja annak biztosítása, hogy egy adott hálózatra vagy számítógépbe ne történhessen illetéktelen behatolás. A tűzfalak általában folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek és felhasználók azonosítóit, a rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak. A tűzfal megpróbálja a privát hálózatot, illetve a hálózati szegmenst a nem kívánt támadásoktól megóvni. Szabályozza a különböző megbízhatósági szintekkel rendelkező számítógép-hálózatok közti forgalmat.

**Változáskezelés:** azon szabályok összessége, amelyek meghatározzák egy informatikai alkalmazás adatszolgáltatási folyamataiban, az azokat kiszolgáló informatikai eljárásokban és szolgáltatásokban, valamint az alkalmazás üzemeltetését lehetővé tevő informatikai infrastruktúrában bekövetkező módosítások, változások biztonságos végrehajtását és nyilvántartását, változásainak nyomon követhetőségét.

**Védelmi rendszer:** a védelmi rendszer az informatikai rendszer megfelelő szintű biztonságának garantálása érdekében alkalmazott fizikai-, logikai- és adminisztratív védelmi intézkedések összessége.

**Kártékony kódok (malware):** olyan rosszindulatú számítógépes program vagy programtörzs (pl.: vírus, trójai zsarolóvírus, kémprogram stb.), amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl.: konkrét időpont, szabad lemezterületi helyek száma stb.) trójai faló hatást indít el.

**Vírusvédelmi rendszer:** a vírusvédelmi rendszer és a hozzá kapcsolódó védelmi mechanizmusok feladata az informatikai rendszerhez kapcsolódó rosszindulatú számítógépes programok (például vírusok) felkutatása, működésük, aktív vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint – megsemmisítésük.

**Visszaállítási eljárás:** olyan eljárásrend, amelynek részeként elvégzett tevékenységek, feladatok biztosítják, hogy a helyreállítási eljárással beindított informatikai szolgáltatás alternatívájáról az ügyviteli folyamat visszaáll a normál üzemmenetre.

**VPN:** Virtual Private Network. A virtuális magánhálózat a magánhálózat kiterjesztése, amely megosztott vagy nyilvános hálózatokon (például interneten) keresztüli kapcsolatokat tartalmaz. Virtuális magánhálózattal úgy lehet adatokat küldeni két számítógép között, mintha a két gép közvetlen kapcsolatban lenne egymással. A VPN kapcsolatok segítségével a szervezetek földrajzilag különálló irodákkal vagy más szervezetekkel is létesíthetnek kapcsolatot úgy, hogy a kommunikáció biztonságos maradjon.

**Zárt védelem:** az összes számításba vehető fenyegetést figyelembe vevő védelem.

**PTE Informatikai Biztonsági Szabályzat 2. számú melléklet**

Kapcsolódó jogszabályok, szabályozások listája

# 1. Jogszabályi háttér

## 1.1. Jogszabályok

- Magyarország Alaptörvénye VI. cikk
- 1997. évi CLIV. törvény az egészségügyről
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2011. évi CXC. törvény a nemzeti köznevelésről
- 2011. évi CCIV. törvény a nemzeti felsőoktatásról (Nftv.)
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi LXXVII. törvény a felnőttképzésről
- 2015. évi CXLIII. törvény a közbeszerzésekről
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 2019. évi LXXX. törvény a szakképzésről

## 1.2. Uniós jogszabályok

- Az Európai Parlament és az Európai Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
  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)

## 1.3. Kormányrendeletek

- 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 451/2016. (XII. 19.) Korm. rendelet - az elektronikus ügyintézés részletszabályairól
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

- 41/2015. (VII. 15.) BM rendelet 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 (Hatályos: 2024.12.31-ig)
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól
- 7/2024. (VI. 24.) SZTFH rendelete a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről
- 7/2024. (VI. 24.) MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

**2. Kapcsolódó belső szabályozások**

- A Pécsi Tudományegyetem Szervezeti és Működési Szabályzata (PTE SZMSZ);
- A PTE SZMSZ 4. számú melléklete – A Pécsi Tudományegyetem foglalkoztatási követelményrendszere;
- A PTE SZMSZ 32. számú melléklete - A Pécsi Tudományegyetem igazgatásának szervezetére vonatkozó szabályzata;
- A PTE SZMSZ 37. számú melléklete – A Klinikai Központ szervezeti és működési szabályzata;
- A Pécsi Tudományegyetem Informatikai Szabályzata;
- A Pécsi Tudományegyetem Távközlési Szabályzata;
- 7/2023. számú kancellári utasítás a Pécsi Tudományegyetem belső kontrollrendszerének szabályozásáról;
- A Pécsi Tudományegyetem szabályzata a tanulmányi rendszerről;
- A Pécsi Tudományegyetem Adatvédelmi Szabályzata;
- A Pécsi Tudományegyetem Egészségügyi Adatvédelmi Szabályzata;
- A Pécsi Tudományegyetem a közérdekű adatok nyilvánosságra hozataláról és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló Szabályzata;
- A Pécsi Tudományegyetem Biztonsági Szabályzata;
- A Pécsi Tudományegyetem Tűzvédelmi Szabályzata;
- A Pécsi Tudományegyetem Beszerzési és Közbeszerzési Szabályzata

**3. Kapcsolódó szabványok és ajánlások**

- MSZ EN ISO 9000:2015 Minőségirányítási rendszerek. Alapok és szótár,
- MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Alapok és követelmények,
- ISO/IEC 27000:2014 Information technology - Security techniques – Information security managements systems. Overview and vocabulary,
- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények,
- MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek,
- ITIL. (Information Technology Infrastructure Library) informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló kormányzati ajánlás, „de facto” szabvány.
- a MABISZ biztonságtechnikai ajánlása B/I. pontja szerinti teljes mechanikai, fizikai védelem;
- a MABISZ biztonságtechnikai ajánlása C/I/2. pontja szerinti részleges elektronikai jelzőrendszer;
- a MABISZ biztonságtechnikai ajánlása C/II. pontja szerinti beléptető rendszer.

**PTE Informatikai Biztonsági Szabályzat 3. számú melléklet**

Információbiztonsági Politika

A Pécsi Tudományegyetem (továbbiakban: PTE) a Dél-Dunántúli régió meghatározó felsőoktatási intézménye, mely komoly múlttal és tradíciókkal rendelkezik, ugyanakkor a jövőben regionális szinten vezető, országos szinten meghatározó, nemzetközi szinten mértékadó szereplővé kíván válni.
Ennek elengedhetetlen feltétele – összhangban Magyarország Nemzeti Kiberbiztonsági Stratégiájával – az adatvagyon, az elektronikus információs rendszerek magas szintű védelme, a kiberbiztonsági elemek fokozottabb implementációja. A PTE alaptevékenységei – úgy, mint az oktatás, a tudományos kutatás, a művészeti alkotótevékenység, a gyógyítás, – által, létfontosságú rendszerelem üzemeltetőként az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozik, ezért minden szervezeti egységének és munkavállalójának alapvető érdeke a biztonságos és megbízható kibertéren belül az informatikai rendszerek és rendszerelemek folyamatos működési biztonságának megvalósítása, megerősítése.
Információbiztonság szempontjából a technikai védelmi megoldások mellett a PTE nagy hangsúlyt fektet a felhasználói tudatosság információbiztonság szempontjából történő fejlesztésére is, tekintettel arra, hogy a támadók a rendszerek sérülékenységeit kihasználva egyre nagyobb mértékben veszik célba a felhasználót.

## 1. Célkitűzés

Jelen Információbiztonsági Politika célja magas szinten támogatni (és szabályozni) a PTE alapfeladatainak zavartalan ellátásához szükséges információbiztonsági alapelveket, hogy mind a rendszerek állapotát, mind a bekövetkezett biztonsági eseményeket figyelemmel lehessen kísérni egységes módon, központilag.

## 2. Alapelvek

A PTE az informatikai biztonság területén az alábbi alapelveket érvényesíti:

1. **Bizalmasság:** az elektronikus információs rendszerekben tárolt információkat csak az arra jogosultak és csak a jogosultsági szintjüknek megfelelően ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásukról.

2. **Sértetlenség:** 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 kizárólag rendeltetésének megfelelően használható.

3. **Rendelkezésre állás:** az elektronikus információs rendszerek az arra jogosult számára elérhetőek és az abban kezelt adatok felhasználhatók.

4. **Védelem teljeskörűsége:** jelen elvet a fizikai-logikai és az adminisztratív védelem területén három dimenzióban kell megvalósítani:
    a. az összes rendszerelemre;
    b. a rendszerek architektúrájának valamennyi rétegére, alkalmazások és infrastruktúra területén egyaránt;
    c. a központi, illetve a végponti informatikai eszközökre és környezetükre.

5. **A védelem zártsága:** az összes valószínűsíthető fenyegetés ellen megelőző védelmi intézkedések megvalósításra kerültek és azok szabályozott, szerves egységet alkotnak.

6. **A védelem kockázatarányossága:** az elektronikus információs rendszer olyan védelme, amelynek során - egy kellően nagy időintervallumban - a védelem költségei arányosak a

fenyegetések által okozható károk értékével. Célkitűzés a minimális költséggel elért maximális védelmi képesség.

–

7. **A védelem folytonossága:** a kialakított védelmi intézkedések az időben állandóan változó biztonsági környezet és viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

A PTE az információbiztonsági védelmi intézkedések megvalósítása során mind az információbiztonsági szabályozás kialakítása, mind a napi operatív intézkedések során három, egymásra épülő és egymást kiegészítő kontrollra épít, továbbá figyelembe veszi, hogy a lehetséges veszélyek teljes kizárása lényegében lehetetlen, így a veszélyek feletti kontrollra fókuszál.

A beépített biztonsági kontrollok az alábbiak:

a) preventív (megelőző) kontroll;
b) detektív (észlelő) kontroll;
c) korrektív (elhárító) kontroll.

A PTE a fenti alapelvek figyelembevételével tervezte meg, alakította ki, működteti és fejleszti információbiztonsági szabályozását és folyamatait annak érdekében, hogy a kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus rendszerek elemeinek rendelkezésre állását, sértetlenségét veszélyeztető mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek teljes életciklusára kiterjedő védelmét biztosítsa logikai, fizikai, és adminisztratív védelmi intézkedések bevezetésével.

A PTE minden munkatársának, szerződéses partnerének elemi érdeke és kötelessége az információbiztonsági szempontok figyelembevétele és az információbiztonsági szabályozások betartása, ennek érdekében folyamatosan növeli és fejleszti a munkavállalók biztonságtudatossági szintjét.

| Rendszer | Felelős | Biztonsági osztály |
|---|---|---|
| Neptun Egységes tanulmányi rendszer | IIG | 4 |
| eMedSolution Kórházi információs rendszer (HIS) | KK | 4 |
| Aspyra PACS Medikai képtároló és továbbító rendszer | KK | 3 |
| SAP Integrált vállalatirányítási rendszer (ERP) | IIG | 3 |
| Nexon Bér- és humánügyviteli információs rendszer | IIG | 4 |
| Poszeidon irat és dokumentumkezelő rendszer | IIG | 3 |
| PTE KPVK Informatikai rendszer | KPVK | 3 |
| PTE BTK web szerverek | BTK | 3 |
| GLIMS laboratóriumi információs rendszer | KK | 4 |
| Corvina integrált könyvtári rendszer | EKTK | 3 |
| Központi DNS szolgáltatás | IIG | 3 |
| Alkörzeti DNS szolgáltatás | Alegységek | 3 |
| Vezetékes számítógép hálózat | IIG | 3 |
| Moodle e-Learning CMS | IIG | 2 |
| Egyetemi PSTN és VoIP távközlési rendszer | IIG | 2 |
| Eduroam vezeték nélküli számítógép hálózat | IIG | 2 |
| Egyetemi levelező rendszer | IIG | 3 |
| Alegységek levelező rendszerei | Alegységek | 3 |
| Alegységek oktatástámogató információs rendszerei | Alegységek | 2 |
| Egészségügyi informatikai támogató rendszerek | KK | 3 |
| Központi portál rendszer | IIG | 2 |
| Kutatás támogató információs rendszerek | Alegységek | 2 |
| Microsoft 365 felhő alapú információs rendszer | IIG | 3 |
| Központi Active Directory címtárszolgáltatás | IIG | 3 |
| Nagios hálózati és rendszer monitorozó infrastruktúra | IIG | 4 |
| Fizikai és logikai riasztó és megfigyelő rendszerek | Alegységek | 2 |
| Központi fájl szerverek, tárolórendszerek | IIG | 3 |
| Központi virtualizációs környezet | IIG | 3 |
| Határvédelmi rendszerek | IIG | 4 |
| Központi adatbázis szolgáltatás | IIG | 3 |
| Egyetemi Vezetői Információs Rendszer (VIR) | IIG | 2 |
| Medbakter mikrobiológiai informatikai rendszer | KK | 4 |
| Foglalkozás-egészségügyi nyilvántartó rendszer | KK | 3 |
| Időszerver szolgáltatás | IIG | 3 |
| Alegységek egyéb informatikai rendszerei és szolgáltatásai | Alegységek | 2 |
| PTE Service Manager | IIG | 2 |
| CATO | KK | 3 |
| POCT (Point of Care Testing) | KK | 3 |

**PTE Informatikai Biztonsági Szabályzat 5. számú melléklet**

Szervezetek biztonsági szintbe sorolása

| Szervezet/Szervezeti egység | Biztonsági szint |
|---|---|
| Pécsi Tudományegyetem általános besorolás | 3 |
| Klinikai Központ általános besorolás | 3 |
| Szőlészeti és Borászati Kutatóintézet | 2 |
| Pécsi Tudományegyetem<br>Informatikai és Innovációs Igazgatóság | 4 |

**PTE Informatikai Biztonsági Szabályzat 6. számú melléklet**

Adatosztályozó lap

| | | |
|---|---|---|
| **Adatgazda:**<br>(név, beosztás) | | |
| **Szervezeti egység:** | | |
| **Adatcsoport megnevezése (rendszer):** | | |

| **Az adatcsoport rövid leírása (célja, funkciója, rendeltetése):** |
|---|
| |

| **Osztályozás:** | |
|---|---|
| Bizalmasság és sértetlenség szempontjából (Nyilvános, Belső, Bizalmas, Titkos) | |
| Rendelkezésre állás szempontjából<br>(1-5 skála) | |

Dátum: ……,

……

Adatgazda

## KITÖLTÉSI ÚTMUTATÓ

**Adatbiztonsági kategóriák:**

| Adatbiztonsági kategória (Hozzáférés) | Jelölés | Tárolás | Továbbítás | Megsemmisítés |
|---|---|---|---|---|
| Nyilvános adatok | Jogszabály által nem védett adatok | Nincsen speciális követelmény, bármilyen adathordozón, titkosítatlan formában tárolható. | Nincsen speciális követelmény, szabadon továbbítható. | Nincsen speciális követelmény, speciális megsemmisítést nem igényel. |
| Belső | A védett adatokat tartalmazó adathordozókat „Belső használatra” kell ellátni. | Az adathordozókat zárható helyiségben kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés vezérlését. | Szervezeten belüli továbbítása hozzáférési jogosultság függvényében engedélyezett. Szervezeten kívülre való továbbítása csak a vezető adatgazda engedélyével lehetséges az elfogadott titkosítási módszer alkalmazásával. | Megsemmisítés az adatgazda engedélyével. Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell. |
| Bizalmas | A bizalmas adatokat tartalmazó adathordozókat „Bizalmas” jelöléssel kell ellátni. | Az adathordozókat zárható helyen szekrényben, vagy zárható asztalfiókban kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés vezérlését. | Szervezeten belüli továbbítása hozzáférési jogosultság függvényében engedélyezett. Szervezeten kívülre való továbbítása csak a vezető adatgazda engedélyével lehetséges az elfogadott titkosítási módszer alkalmazásával. | Megsemmisítés a vezető adatgazda engedélyével. Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell. |

| | | | | |
|---|---|---|---|---|
| Titkos | A titkos, illetve fokozottan védett adatokat tartalmazó adathordozókat „Titkos” jelöléssel kell ellátni. | A titkos, illetve fokozottan védett adatokat tartalmazó adathordozókat páncélszekrényben kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés hitelesítésen alapuló vezérlését. | Titkos, illetve fokozottan védett adatokat csak titkosított csatornán, hitelesített felhasználónak szabad küldeni, vagy csak helyi hozzáférés lehetséges. | Megsemmisítés az adatgazda külön engedélyével. Megsemmisítés előtt az adathordozón levő adatokat visszaállíthatatlanul törölni kell. |

Azon adatok, amelyek egyértelműen máshova nem kerültek besorolásra, azok belső kategóriába tartoznak.

Az információrendszerben elektronikusan tárolt adatok esetén az adatok azon halmazát, amelyekre a tárolás körülményeiből adódóan jellemzően azonos védettség valósítható meg (közös adatbázis, azonos könyvtár), ugyanabba az adatbiztonsági osztályba kell sorolni, mégpedig oly módon, hogy a halmaz egészére ki kell terjeszteni a halmaz legérzékenyebb elemének besorolását, vagy a különböző adatbiztonsági osztályokba sorolható adatokat külön kell bontani.

Az Egyetem egyes folyamatai, szervezeti egységei nevében, az általuk használt adatok vonatkozásában az Adatgazdák határozzák meg az adat besorolási/adatosztályozási kategóriákat.

Az Egyetem informatikai rendszerében az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosításáért az IIIG Igazgatója a felelős.

**Rendelkezésre állás szempontjából kategóriák:**

| **Biztonsági osztály** | **Leírás** |
|---|---|
| **1** | 2.2. Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel<br>2.2.1. az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;<br>2.2.2. nincs bizalomvesztés, a probléma azérintett szervezeten belül marad, és azon belül meg is oldható;<br>2.2.3. a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen; |
| **2** | 2.3. A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel<br>2.3.1. személyes adat sérülhet;<br>2.3.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat vagy elektronikus információs rendszer sérülhet;<br>2.3.3. a lehetséges társadalmi-politikaihatás az érintett szervezeten belül kezelhető;<br>2.3.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át. |
| **3** | 2.4. A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel<br>2.4.1. különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;<br>2.4.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet;<br>2.4.3. a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;<br>2.4.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át. |
| **4** | 2.5. A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel<br>2.5.1. különleges személyes adat nagy mennyiségben sérülhet;<br>2.5.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);<br>2.5.3. az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;<br>2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni; |

| | |
|---|---|
| | 2.5.5. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át. |
| **5** | 2.6. Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel<br>2.6.1. különleges személyes adat kiemelten nagy mennyiségben sérülhet;<br>2.6.2. emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következik be<br>2.6.3. a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;<br>2.6.4. az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;2<br>.6.5. a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;<br>2.6.6. az érintett szervezet üzlet-vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;<br>2.6.7. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át. |

**PTE Informatikai Biztonsági Szabályzat 7. számú melléklet**
IBSZ eljárásrendjei

1. Adathordozók védelmére vonatkozó eljárásrend
2. Azonosítási és hitelesítési eljárásrend
3. Biztonsági esemény- és incidenskezelési eljárásrend
4. Biztonságos fejlesztési követelmények eljárásrendje
5. Biztonságtervezési eljárásrend
6. Hozzáférés védelmi és jogosultságkezelési eljárásrend
7. Fizikai védelmi intézkedések eljárásrendje
8. Információbiztonsági kockázatok kezelésének eljárásrendje
9. Informatikai beszerzési eljárásrend
10. E-mail és internet használati eljárásrend
11. Üzletmenet- folytonosság és katasztrófa elhárítási eljárásrend
12. IT biztonsági kockázatelemzési és kockázatkezelési eljárásrend
13. Konfigurációkezelési eljárásrend
14. Kriptográfia és kulcs menedzsment eljárásrend
15. Mentési és archiválási eljárásrend
16. Mobil eszközök használatának eljárásrendje
17. Naplózási és naplóelemzési eljárásrend
18. Rendszer- és kommunikációvédelmi eljárásrend
19. Rendszer karbantartási eljárásrend
20. Személybiztonsági eljárásrend
21. Távoli hozzáférés engedélyezési, használati eljárásrend
22. Vírus- és kártékony kód elleni védelem eljárásrendje
23. Adatok biztonsági osztályba sorolása és kezelése eljárásrend
24. Fejlesztések során követendő minimális biztonsági intézkedések eljárásrendje
25. WEB szerveren történő adattárolás, domain nevek használatának, tanúsítványok igénylésének eljárásrendje