# 1/2010. sz. Gazdasági Főigazgatói Utasítás a PTE rendszereihez nyújtott hozzáférés és jogosultságkezelés szabályozásáról

# 1. Dokumentum adatlap

| **Azonosítás** | |
|---|---|
| Dokumentum címe | 1/2010. sz. Gazdasági Főigazgatói Utasítás a PTE rendszereihez nyújtott hozzáférés és jogosultságkezelés szabályozásáról |
| Állomány neve | Hozzaferes es jogosultsagkezeles utasitas.docx |
| Dokumentum verzió | 1.0 |
| Kiadás időpontja | 2010.03.31. |
| Hatályba lépés időpontja | 2010.03.31. |
| Készítette | Ripli Péter |
| Ellenőrizte | Vukovics Mihály |
| Jóváhagyta (IIG) | Sári Csaba |

# 2. Tartalomjegyzék

**1. Dokumentum adatlap ..... 2**
**2. Tartalomjegyzék ..... 3**
**3. Tevékenység ..... 5**
**4. Cél ..... 6**
**5. Felelősség ..... 7**
**6. Kontroll pontok ..... 8**
*6.1. Folyamat minőségi jellemző ..... 8*
**7. Az utasítás hatálya ..... 9**
*7.1. Szervezeti hatály ..... 9*
*7.2. Személyi hatály ..... 9*
*7.3. Tárgyi hatály ..... 9*
**8. A hozzáférés ellenőrzés szervezeti működési követelménye ..... 10**
*8.1. Zárt rendszer ..... 10*
*8.2. Publikus rendszer ..... 10*
*8.3. Hozzáférés ellenőrzési politika ..... 10*
**9. Felhasználói hozzáférés kezelése ..... 11**
*9.1. Felhasználók hozzáférésének nyilvántartása ..... 11*
*9.2. Jogosultságok igénylése ..... 11*
*9.3. Jogosultságok módosítása ..... 11*
*9.4. Jogosultságok visszavonása ..... 11*
*9.5. Rendszer-, alkalmazás adminisztrátori jogosultságok kezelése ..... 12*
*9.6. Átmeneti jogosultságok kezelése ..... 12*
*9.7. Felhasználói hozzáférési jogosultságok átvizsgálása ..... 12*
**10. Hálózati szintű hozzáférés ellenőrzés ..... 13**
*10.1. Hálózati szolgáltatások használatára vonatkozó politika ..... 13*
10.1.1. A szabályozás szervezeti hatálya ..... 13
*10.2. Felhasználó hitelesítés külső kapcsolatok esetén ..... 13*
*10.3. Távdiagnosztikai port védelme ..... 13*
*10.4. Elkülönítés a hálózatokban ..... 13*
*10.5. Hálózathoz való csatlakozás felügyelete ..... 14*
**11. Operációs rendszer szintű hozzáférés ellenőrzés ..... 15**
*11.1. Automatikus terminál azonosítás ..... 15*
*11.2. Terminálon való bejelentkezés eljárásai ..... 15*
*11.3. Felhasználó azonosítása és hitelesítése ..... 15*
*11.4. Jelszókezelő rendszer ..... 15*

*11.5. Kényszerjelzés a felhasználók védelmére ..... 15*
*11.6. Kapcsolati idő korlátozása ..... 15*
11.6.1. Jelenleg időkorlátozást alkalmazunk a következő területen ..... 15
**12. Alkalmazás szintű hozzáférés ellenőrzés ..... 17**
*12.1. Információ – hozzáférés korlátozása ..... 17*
*12.2. Érzékeny rendszerek elkülönítése ..... 17*
**13. Rendszerhozzáférés és használat figyelemmel követése ..... 18**
*13.1. Esemény naplózás ..... 18*
*13.2. Órajel szinkronizálás ..... 18*

## 3. Tevékenység

Az informatikai rendszerekhez és az általuk tárolt adatokhoz való hozzáférések szabályait határozza meg a hozzáférés és jogosultságkezelés menedzsment utasítás.

## 4. Cél

Az adatokhoz való jogosulatlan/illetéktelen hozzáférés megakadályozása és a jogosult hozzáférések kezelése, nyilvántartása.

## 5. Felelősség

A hozzáférési szintek besorolása a szakterületi Osztályvezetők feladata.
Az informatikai jogosultság igényeket az felhasználó vezetőjének és az erőforrás IT oldali gazdájának is jóvá kell hagyni.

# 6. Kontroll pontok

- A hozzáférési jogosultságok szabályozásának megléte külső és belső felhasználók részére
- Adminisztrátori jogosultságok körének megléte
- A munkakörhöz kapcsolódó jogosultságok halmazának megléte és karbantartása
- A munkakörhöz kapcsolódó szoftver eszközök halmazának megléte és karbantartása
- Átmeneti jogosultságok kezelésének megléte
- Informatikai rendszerek és a jogosultság nyilvántartó rendszerek, adatbázisok, felhasználó hozzáférési jogosultságok összehasonlítása, különbségek elemzése, szinkronizálás végrehajtása (negyedévenkénti ellenőrzés)

## 6.1. Folyamat minőségi jellemző

- Hozzáférési jogosultságok kapcsán adódó biztonsági incidensek száma
- A jogosultság nyilvántartó rendszer és a produktív rendszerekben beállított jogosultságok közti eltérés

# 7. Az utasítás hatálya

## 7.1. Szervezeti hatály

A jelen utasítás hatálya kiterjed a PTE minden szervezetei egységére.

## 7.2. Személyi hatály

Az utasítás személyi hatálya kötelező érvénnyel kiterjed a PTE minden közalkalmazottjára. Az utasításban foglaltak érvényesülését a partner szerződések tartalmának megfelelő kialakításával is biztosítani kell.

## 7.3. Tárgyi hatály

Az utasítás tárgyi hatálya kiterjed a PTE által használt valamennyi informatikai rendszerre.

# 8. A hozzáférés ellenőrzés szervezeti működési követelménye

A Pécsi Tudományegyetemen (PTE) alapvetően kétféle rendszert különböztetünk meg, a zárt- és a publikus elérést. A rendszer elérések a jogosultság kezelés és elérés szempontjából a következők:

## 8.1. Zárt rendszer

A PTE-n használt belső informatikai rendszerek, amelyek lehetnek:

- Belső hozzáférés alapúak: itt az elérés csak a belső saját hálózatról lehetséges.
- Külső hozzáférés alapúak: minden olyan elérés, melyet bármilyen külső hálózatról kezdeményeznek. Itt a külső hozzáférési jogosultságot az Infrastruktúra Üzemeltetési Osztály és az Adatbiztonság Felelős határozza meg.

## 8.2. Publikus rendszer

A PTE azon rendszereit takarja, melyeket az Internet felől el lehet érni titkosított csatorna kiépítése nélkül. Ebben az esetben is két további rendszert különböztetünk meg:

- Teljesen publikus rendszer
- Hallgató, „ügyfél” által elérhető rendszer: csak regisztrált partnerek érhetik el.

## 8.3. Hozzáférés ellenőrzési politika

A PTE-n használt rendszer jogosultsági felépítését a lehető legbiztonságosabb módon kell megoldani. Az alap megállapítás, hogy mindenki a lehető legkevesebb, számára még szükséges jogosultsággal rendelkezzen.

**A PTE hozzáférési rendszerének alapját a kialakított munkakörök képezik.** Minden egyes munkakörhöz meg kell állapítani a szükséges szoftver eszközöket és jogosultságokat. További jogosultságok adása csak indokolt esetben, a szervezeti egység vagy a felettes osztályvezető engedélyével és az erőforrás felelősének jóváhagyásával lehetséges. Külső személyek hozzáférési jogai a „Külső partnerek távoli hozzáférése a PTE rendszereihez utasítás” kapcsolódó dokumentumban van részletezve.

# 9. Felhasználói hozzáférés kezelése

## 9.1. Felhasználók hozzáférésének nyilvántartása

A jogosultságokat az igénylés pillanatától dokumentálni kell. Egy dokumentációs rendszerben felhasználónként nyilván kell tartani a jogosultságok igénylésének, megadásának, visszavonásának tényét.

A PTE rendszerei, adatátviteli vonalai és alkalmazásai csupán az Egyetem oktatási, gyógyítói, kutatói és ügyviteli tevékenységének elősegítésére használhatóak, így a felhasználók IT tevékenységeit az Egyetem felhatalmazott szakemberei bármikor ellenőrizhetik. **A Felhasználókat erről a tényről minden bejelentkezéskor értesíteni kell.**

## 9.2. Jogosultságok igénylése

Új felhasználó belépésekor a munkakörének megfelelő jogosultsági csoport beállításával korlátozzuk az adatok, információk és erőforrások használatát a felhasználó számára úgy, hogy a munkaköri feladatainak ellátásához szükséges mértékű legyen.

A belső rendszerek eléréséhez jogosultságot egy felhasználó csak akkor kaphat, ha rendelkezik ETR azonosítóval.

Az ETR azonosítóval rendelkező felhasználó felettes vezetője – külső felhasználó esetén a kapcsolattartó vezetője - a ServiceDesk osztályon keresztül igényli meg a munkaköri jogosultságokat. A felhasználó informatikai jogosultságai a munkaköréhez és egyéb a szervezeti vezetője által megjelölt egyetemi folyamatokhoz kapcsolódó tevékenységek ellátásához szükségesek. A munkakör ellátásához szükséges jogosultságok automatikusan a vezetői jóváhagyást követően biztosítottak, az egyedi jogosultság igények elbírálása a szokásos elbírálási procedúrán megy keresztül (igény felvétel (ServiceDesk), jóváhagyás (felhasználó szervezeti vezetője vagy projekt vezetője), felülvizsgálat (erőforrás gazda Infrastruktúra Üzemeltetési Osztály, Ügyviteli Alkalmazások Osztály) és jogosultság adminisztráció (ServiceDesk).

Alárendelt hozzáférések esetén a felsőbb szintű hozzáférés tulajdonos felelős az alárendelt erőforrás minden jogosultságáért.

## 9.3. Jogosultságok módosítása

Jogosultság módosítási kérelmet az érintett felhasználó vagy szervezeti vezetője (általában osztályvezető) a ServiceDesk Osztályon keresztül jelenthet be. Jogosultságot egy munkatárs részére csak a szervezeti vezetője és esetleges projekt vezetője által jóváhagyott tevékenységek ellátásához lehet kérni. Ennek megítélése az osztályvezető – projekt vezető feladata.
Áthelyezés (területi és/vagy munkaköri) esetén az érintett felhasználó azon jogosultságait, amelyek az új munkaköréhez nem szükségesek a ServiceDesk Osztály törli, és felveszi az új munkakör ellátáshoz szükséges jogosultságokat. A ServiceDesk Osztály a jogosultságok rendezését az áthelyezendő munkatárs új szervezeti vezetőjének kezdeményezésére hajtja végre.

## 9.4. Jogosultságok visszavonása

Amikor a dolgozó munkaviszonya vagy egy korábban ellátott tevékenysége megszűnik, a saját és az általa felügyelt számítógépes hozzáféréseknek 24órán belül letiltásra kell kerülnie.
Munkaviszony megszűnésekor a jogosultságok, az azonosítók törlésével, tiltásával azonnal megszűnnek. A tevékenység megszűnésével, a jogosultság visszavonás a felhasználó szervezeti vezetője vagy a projekt vezetője által a ServiceDesk Osztályon keresztül van indítva.

Az Adatbiztonság Felelős által súlyosnak ítélt – bizalmas, szigorúan bizalmas adatokat sértő, illetve veszélyeztető - informatikai biztonsági incidens esetén, amely szándékos károkozásból, illetve a felhasználó hozzá nem értéséből, tudatlanságából származik - külső és belső személy esetében egyaránt - az incidenst előidéző személy jogosultságait korlátozni kell. A biztonsági incidenssel kapcsolatos eljárást a ServiceDesk Osztály, vonatkozó szabályzatában kell részletezni.

## 9.5. Rendszer-, alkalmazás adminisztrátori jogosultságok kezelése

A felhasználói jogosultságok kiadási folyamatánál szigorúbban kell kezelni a kiváltságos jogokat biztosító adminisztrátori jogok megadását.
Az illetéktelen hozzáférések ellen védendő több felhasználós rendszereknél a jogosultságok kiadásának engedélyezési eljárása során pontosan meg kell határozni azokat a rendszerelemeket, - pl. operációs rendszereket, adatbázis-kezelő rendszert, valamint az alkalmazásokat – és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzárendelni.
Az egyéni jogosultságok végső engedélyezését az Informatikai Igazgatóság vezetője végzi.
Az Adminisztrátori jogosultságokat egy kapcsolódó külön dokumentumban kell szabályozni és kezelni.

## 9.6. Átmeneti jogosultságok kezelése

A produktív rendszerekhez a fejlesztő nem kaphat magas szintű jogosultságot.
Az informatikai rendszerek működtetése során fellépő bizonyos hibák pontos diagnosztizálásához, olykor esetleg elhárításához átmeneti a munkakörhöz rendelt jogosultsági szinthez képest magasabb jogosultság kiosztására is szükség lehet. Amennyiben, egy kritikus alkalmazás produktív üzemben nem elérhető, az Infrastruktúra Üzemeltetés képtelen a hibát kezelni, a fejlesztőnek vagy külső támogatónak kell adni átmeneti ideig a normál jogosultsághoz képest magasabb jogosultságot. Ezeket a jogosultság igényeket minden esetben a ServiceDesk Osztályon keresztül kell kérni az Infrastruktúra Üzemeltetési Osztálytól. Az igény lezárása után az ServiceDesk Osztály ismét visszaállítja az eredeti jogosultsági szintet. Extrém esetekben (pl. a ServiceDesk osztály nem elérhető) ettől a folyamattól el lehet térni azonban utólag mindenféleképpen dokumentálása kötelező.
Ezeket az igényeket kontrollálás céljából negyedévente egyszer átadja az Adatbiztonság Felelősnek a ServiceDesk Osztály vezetője.

Ezen esetek meghatározása és kezelésének a módja (ki adhat jogosultságot és hogyan, dokumentálás módja, érvényesség ideje, visszavonás módja) az Adatbiztonság Felelős és az érintett rendszertulajdonos felelőssége.

## 9.7. Felhasználói hozzáférési jogosultságok átvizsgálása

A jogosultságok, hozzáférések nyilvántartását egy jogosultság kezelő rendszer adatbázisban szükséges nyilvántartani. A jogosultság kezelő rendszer naprakészségéért a megfelelő rendszertulajdonosok felelnek. Ezeknek az adatbázisoknak és az élő jogosultsági rendszernek az összevetését negyed évente el kell végezni, és a nyilvántartás alapján a jogosultságokat szükség esetén módosítani kell.
Amennyiben eltérés található az adatbázisok között, annak okát ki kell vizsgálni, és meg kell szüntetni. Ezeket a feladatokat az érintett rendszerek rendszertulajdonosai végzik.

# 10. Hálózati szintű hozzáférés ellenőrzés

## 10.1. Hálózati szolgáltatások használatára vonatkozó politika

### 10.1.1. **A szabályozás szervezeti hatálya**

A szabályozás szervezeti hatálya a bevezetésekor csak a Gazdasági Főigazgatóság és a Klinikai Központ területekre terjed ki az oktatás/kutatási területeken való alkalmazása egy későbbi időpontban történik meg.

A hálózati szolgáltatások rendelkezésre állását, az ügymenet zavartalan működése szempontjából, folyamatosan biztosítani kell. Ennek érdekében a következőkről kell gondoskodni:

- csak jogosult felhasználók férhessenek hozzá a hálózat szolgáltatásaihoz. Regisztrálni kell minden sikeres és sikertelen bejelentkezést, vagy bejelentkezési kísérletet,
- a nyitott hálózati portokat, amelyek kívülről szolgáltatásként vannak jelen, nyilván kell tartani, ilyennek tekintjük a tűzfal külső oldaláról jövő kéréseket,
- az aktív hálózati eszközök skálázhatóak, bővíthetőek legyenek, valamint biztosítani kell a dinamikus teljesítmény-eloszlás megvalósulását.

A PTE hálózatát csak egy ponton (a PTE tűzfalán keresztül) lehet elérni kívülről és elhagyni belülről. Kívülről való hozzáférés engedélyezése csak demilitarizált zónából (DMZ) lehetséges a megfelelő kontrolok kialakítása mellett. Ekkor egyéb védelmi intézkedések meghozatala javasolt (minimális jogosultságok biztosítása, USB-token vagy mágneskártyás azonosítás stb.). Az intézkedéseket az Osztályvezetők, valamint az Adatbiztonsági Felelős javaslata alapján az Informatikai Igazgatóság vezetője hozza meg.
A munkatársak távoli munkavégzését a VPN rendszer az interneten keresztül egy titkosított csatornán át biztosítja. Az Egyetem rendszereinek elérését a felhasználói azonosító alapján beállított VPN jogosultság alapján kell meghatározni. Az Egyetemen lévő belső alhálózatoknak egymástól elkülönítetten belső VPN eléréssel kell működnie.
Az internet felől az egyetemi alhálózatok elérése kizárólag VPN kapcsolaton keresztül történhet melynek módját a jelen szabályozáshoz kapcsolódó *„Külső partnerek távoli hozzáférése a PTE rendszereihez utasítás”* határozza meg.

## 10.2. Felhasználó hitelesítés külső kapcsolatok esetén

A PTE belső informatikai hálózatába kívülről történő felkapcsolódás csak hitelesítéssel történhet.
Kockázat elemzéssel kell meghatározni a szükséges védelmet és a megfelelő hitelesítési módszert.
Távoli felhasználók hitelesítésére kriptográfiai módszereket kell használni. (titkosított VPN kapcsolat, birtokláson alapuló hitelesítő eszköz, vagy tanúsítvány). A felhasználók körét a minimálisan szükséges szintre kell korlátozni.

## 10.3. Távdiagnosztikai port védelme

A távdiagnosztikai portok védelmének kialakítása fontos biztonsági intézkedés, amely a betörési lehetőségek kockázatát csökkenti. Minden diagnosztikai portot nyilvántartásba kell venni, és naplózni kell a használatukat. Fel kell jegyezni, hogy ki, mikor, milyen célból létesített hozzáférést rajtuk keresztül. A nyilvántartás elkészítése, a hozzáférések naplózási módjának meghatározása és a naplózás végrehajtása a rendszertulajdonosok feladata. A nyilvántartás éves felülvizsgálatáról az Adatbiztonsági Felelősnek kell gondoskodnia. Ilyen távdiagnosztikai elérhetőségek lehetnek pl. ssh, VPN. Hálózatmenedzsment létrehozása: működőképesség figyelése, elérhetőség figyelés, távoli konfiguráció hangolás, security management, naplózás.

## 10.4. Elkülönítés a hálózatokban

A PTE informatikai hálózatán egymást befolyásoló tevékenységek több területen is folyhatnak, amelyek elválasztása célszerű. Gazdasági, egészségügyi, pénzügyi stb. menedzsment.

A PTE belső hálózatát (VLAN-ok) tűzfalnak kell elválasztania a többi zónától.

Az alaphálózat, amely a gerincet és az arra csatlakozó, külön nem védett (elsősorban oktatási) hálózatrészeket tartalmazza, tűzfallal (jelenleg) nem védett.

**Jelenleg elkülönítve kezeljük a következő virtuális hálózatokat:**

- **hálózati eszközök managementje (bejárás más hálózatok felől kizárólag VPN-nel, kijárat még tűzfalkapcsolattal sincs)**
- **ip telefonok és telefonközpont-közi ip kapcsolatok hálózata (ez technikai okok miatt ugyanaz) (bejárás más hálózatok felől kizárólag VPN-nel, üzemeltetési hibakeresési célból)**
- **Gazdasági hálózat (más hálózatoktól tűzfallal leválasztva, bejárás VPN vagy biztonságos WiFi használatával) – de ez a VLAN ugyanakkor több telephelyen is megjelenhet.**
- **WiFi eszközök WLAPP forgalma**
- **Biztonsági kamerarendszer ip alapú forgalma (bejárás a biztonságtechnikai osztály megfigyeléssel megbízott dolgozói részére VPN-nel)**
- **ETR belső hálózat (hozzáférés VPN-nel, üzemeltetési célból)**
- **Klinikai hálózat (külön tűzfallal leválasztva más hálózatoktól) ill. ennek VLAN ágai, melyek a nyilvános hálózatrészen keresztül**
- **authentikált kollégiumi hálózat (helyszíni hozzáférés csak 802.1x autentikációval, külső hozzáférés nincs, tűzfallal védett)**

A felsorolt VLAN-ok esetében az elkülönítés a hozzáférés-szabályozás szempontjából lényeges.

## 10.5. Hálózathoz való csatlakozás felügyelete

A megosztott hálózatok hozzáférését szabályozni, a felhasználók felkapcsolódási lehetőségeit korlátozni kell.
A hálózati forgalom ellenőrzésére szolgálnak:

- a tűzfalak naplói,
- hálózat figyelő és IDS szoftverek,
- belső hálózat szervereinek naplói,
- hálózati eszközök naplói,
- hálózati menedzsment eszközök naplói.

# 11. Operációs rendszer szintű hozzáférés ellenőrzés

## 11.1. Automatikus terminál azonosítás

Idővel a GF szervezeti területen, majd kiterjesztve a teljes egyetemre automatikus terminálazonosítást kell bevezetni, hogy hitelesítsék a speciális állomások és hordozható felszerelések kapcsolódását. Az automatikus azonosítás egy olyan technika, amit akkor lehet használni, ha az összekapcsolódást csak egy meghatározott állomásról, vagy számítógép kliensről tudják csak elindítani. Az Adatbiztonság Felelős és az Infrastruktúra Üzemeltetési Osztályvezető feladata meghatározni azon informatikai eszközök körét, melyeknél a felhasználó azonosításán kívül, az informatikai eszköz azonosítására is szükség van. Ezen informatikai eszközöket külön nyilvántartásba kell venni, illetve a hálózathoz való csatlakozásuk biztonságát félévente ellenőrizni szükséges. A felhasználó és az informatikai eszköz azonosítására is alkalmazható módszer lehet:

- a felhasználó gépéhez rendelt bizonyítvány, illetve titkosító kulcs,
- fizikai cím, DNS, IP szintű ellenőrzés.

## 11.2. Terminálon való bejelentkezés eljárásai

A terminálokra való biztonságos bejelentkezési eljárás megvalósítása erősíti az informatikai biztonság szilárdságát. A bejelentkezési eljárásnak a következő elvekhez kell alkalmazkodnia:

- a bejelentkezés korlátozott időn belül történhet meg,
- három bejelentkezési kísérlet után a rendszernek le kell tiltani a felhasználó bejelentkezési lehetőségét,
- naplózni kell a bejelentkezési kísérleteket,
- téves bejelentkezés során a hibaüzenet nem árulhat el több információt, mint aminek tudására a felhasználó jogosult.

## 11.3. Felhasználó azonosítása és hitelesítése

Minden felhasználónak, kizárólag személyes használatra szóló, egyedi azonosítóval kell rendelkeznie, de egy felhasználónak több azonosítója is lehet.
A felhasználói azonosító - lehetőség szerint - ne utaljon a felhasználó privilégiumára. (például: adminisztrátor)

## 11.4. Jelszókezelő rendszer

A jelszókezelés eljárás rendje kidolgozás alatt van egy külön dokumentumban lesz megtekinthető.

## 11.5. Kényszerjelzés a felhasználók védelmére

A felhasználó jelszó érvényességi idejének lejártakor a rendszer figyelmeztesse a felhasználót a jelszava megváltoztatására. A jelszó képzés szabályait a rendszernek ki kell kényszerítenie.

## 11.6. Kapcsolati idő korlátozása

A PTE alkalmaz kapcsolati időkorlátozást az informatikai rendszerein pl. a külső partnereknek az Egyetem rendszereibe történő bejelentkezése esetében.

### 11.6.1. **Jelenleg időkorlátozást alkalmazunk a következő területen**

Egyetemi konferencia idejére kiadott résztvevői WiFi hozzáférés a PTE-CONFERENCE WiFi szolgáltatásra. A kiadott közös azonosító/jelszó a konferencia szervezője által megadott rendezési időtartamra él, az időkorlát az azonosító bejegyzésével egyidejűleg kerül rögzítésre és beavatkozás nélkül automatikusan lejár.

Továbbiakban a *„Külső partnerek távoli hozzáférése a PTE rendszereihez utasítás”* rendelkezik még a kapcsolati idő korlátozásról.

# 12. Alkalmazás szintű hozzáférés ellenőrzés

## 12.1. Információ – hozzáférés korlátozása

A felhasználói rendszerekhez való hozzáférést oly mértékben kell korlátozni, hogy a felhasználó a munkaköréhez szükséges feladatokat el tudja látni, de ne legyen lehetőség a munkájához nem tartozó információkba való betekintésre vagy beavatkozásra.

Ez több módon elérhető:

- bejelentkezési eljárás definiálása,
- következtetési lehetőség kizárása, azaz a rendszer jelzés, vagy figyelmeztetés ne szolgáltasson többlet információt,
- hozzáférések naplózása.

## 12.2. Érzékeny rendszerek elkülönítése

Érzékeny adatnak nevezzük azokat az adatokat, amelyeket az adatosztályozás során bizalmasnak, vagy szigorúan bizalmasnak ítéltek meg.
Ezen adatokat védeni kell a jogosulatlan hozzáféréstől. Védelmük fizikai és logikai védelemmel oldható meg.

A fizikai védelem lehetőségei:

- Az adatokat kezelő rendszer tényleges elkülönítése történhet:
  - fallal, ráccsal határolt helyiségben,
  - beléptető rendszerrel,
  - élőerős védelemmel,
  - riasztóval őrzött helyiségben.
- Az adatok hálózati eszközök segítségével való elkülönítése.

A logikai elkülönítés módszerei:

- hozzáférési jogok kialakítása,
- bejelentkezési eljárások definiálása,
- rejtjelezés, titkosítás használata.

Az elkülönítés megtervezése és módszereinek kiválasztása az Adatbiztonság Felelős és az Infrastruktúra Üzemeltetési Osztályvezető feladata.

# 13. Rendszerhozzáférés és használat figyelemmel követése

## 13.1. Esemény naplózás

Az eseménynaplózás előírásait az Üzemeltetési és karbantartási szabályozások között kell szerepeltetni.

## 13.2. Órajel szinkronizálás

A rendszermonitorozás elengedhetetlen feltétele a pontos dátum és időbeállítás, mert csak a pontos időpont tudatában lehet visszakövetkeztetni az eseményekre. Ennek megvalósítása esetleg egy központi time szerverrel javasolt.