

12.b Határozza meg az informatikai biztonság szabályzási és dokumentációs rendszerét, adjon példát az egyes dokumentumok tartalmára intézményi környezetben!

### Mi a szabályozási rendszer?

- Fontos szerepet játszik az intézmények biztonságos és hatékony működésében, mivel biztosítja a szabályok és előírások betartását, megelőzve az esetleges jogi, biztonsági vagy reputációs kockázatokat.
- Az informatikai biztonság szabályzási és dokumentációs rendszere egy olyan strukturált módszer, ami segíti az intézményeket abban, hogy az információik biztonságosan legyenek kezelve és védelmezve legyenek.
  - o A rendszer magában foglalja azokat a szabályokat, folyamatokat, dokumentumokat és eljárásokat, amik az intézmény informatikai rendszerének biztonságához szükségesek.

### ISO/IEC 27001 szabvány

- ISO/IEC 27000 szabványcsalád tagja, ami az information security management system követelményszabványa.
- A szabvány meghatározza azokat a rendszerkövetelményeket, amik célja, hogy az információbiztonság megfelelő felügyelet és ellenőrzés alatt álljon.

### Mikre terjed ki a követelményrendszere?

- Szervezeti biztonság
- Alkalmazottakhoz kapcsolódó biztonság
- Külső személyekhez kapcsolódó biztonság
- Eszközök osztályozása és ellenőrzése
- Kommunikáció és üzemeltetés irányítás
- Hozzáférés ellenőrzés
- Működés folyamatosság irányítás
- Rendszerfejlesztés és karbantartás

### Előnyei

- **Szabályozást ad**
  - o Adatvesztés
  - o Jogosulatlan hozzáférés
  - o Vírustámadás
  - o Illetéktelen behatolás
  - o Katasztrófa elhárítás
- Hozzájárul az információvagyon sérülésének megakadályozásához és a vállalkozás partnerei számára is biztosítékot ad arra, hogy az információkkal kapcsolatos kockázatok kezelése biztosított.



Dokumentumai (ezeken kívül még több is megtalálható, ezek a ténylegesen ajánlottak)

- Belső (Internal) Audit
- Information Security Policy
- Risk Assessment
- Statement of Applicability

#### Internal audit (9.2 Internal Audit)

- Szervezetten belüli auditálás, ellenőrzések.
- **Tartalma**
  - o Executive summary
    - Szervezet megfelelőségi állapot
    - Kezelendő hiányosságok
  - o Audit leírása
    - Információkat kell tartalmaznia az audit elvégzésének módjáról.
  - o Hiányosságok és javítási lehetőségek
  - o Javító (corrective) intézkedések meghatározása

#### Information Security Policy (5.2 Policy)

- Magas szintű áttekintést nyújt arról, hogy a szervezet hogyan közelíti meg az információbiztonságot.
- **Tartalma**
  - o Cél (Purpose)
  - o Követelmények (Requirements)
    - Jogi, szerződéses, szabályozási követelmények
  - o Szerepek és felelősségi körök (Roles & responsibilities)
    - Ki felel a megvalósításért, karbantartásért, monitorozásért az ISMS-en belül.
  - o Kommunikáció (Communication)
    - Szabályzatot kivel kell megosztani (belső vagy külső féllel)

#### Risk Assessment (6.1.2)

- Azonosítják a szervezeti kockázatokat, meghatározzák az egyes kockázatok valószínűségét és hatását, és felvázolják, hogy a szervezet hogyan fog reagálni az egyes kockázatokra.
- **Tartalma**
  - o Kockázatok észlelése
  - o Kockázatok elemzése
    - Veszélyességi szint hozzárendelése
  - o Kockázatok értékelése és rangsorolása
  - o Kockázatkezelési terv kitöltése
  - o Kockázati jelentése készítése

#### Statement of Applicability (6.1.3)

- Az Annex A biztonsági ellenőrzések közül melyek alkalmazhatóak és melyek nem az ISMS-re.
- **Tartalma**
  - o Kockázatkezelés végrehajtása
    - Risk assessment-ből kiindulva
  - o Security kontrollok kiválasztása a kockázatok csökkentésére.
  - o Lista azokról a kontrollokról, amiket nem fogunk használni és miért nem.
    - Nem akarunk nagy összeget költeni egy kis összegű problémára.
  - o Dokumentáció naprakészen tartása.