12.b

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

Mi a szabályzási rendszer?

A szabályzási rendszer fontos szerepet játszik az intézmények biztonságos és hatékony működésében, mivel biztosítja a szabályok és előírások betartását, megelőzve ezzel az esetleges jogi, biztonsági vagy reputációs kockázatokat.

Az informatikai biztonság szabályzási és dokumentációs rendszere egy olyan strukturált módszer, amely segíti az intézményeket abban, hogy az információik biztonságosan legyenek kezelve és védelmezve legyenek. A rendszer magában foglalja azokat a szabályokat, folyamatokat, dokumentumokat és eljárásokat, amelyek az intézmény informatikai rendszerének biztonságához szükségesek.

1. Felhasználói kézikönyv: Ez a dokumentum az informatikai eszközök használatára vonatkozó legfontosabb irányelveket tartalmazza, beleértve a felhasználói fiókok kezelését, az adatok tárolását és a biztonsági szabályokat.
2. Rendszerdokumentáció: Ez a dokumentum az informatikai rendszerek és szolgáltatások részletes leírását tartalmazza, beleértve a rendszer felépítését, a telepített szoftvereket és azok konfigurációját.
3. Rendszerfelügyeleti dokumentáció: Ez a dokumentum az informatikai rendszerek és szolgáltatások működésének felügyeletére vonatkozó részletes eljárásokat tartalmazza, beleértve a rendszeres karbantartást, a mentéseket és a hibaelhárítást.
4. Jogi dokumentumok: Ezek a dokumentumok az adatvédelemre és az információvédelemre vonatkozó jogszabályokat és rendeleteket tartalmazzák. Például az adatvédelmi szabályzat, a felhasználói szerződés vagy az adatvédelmi tájékoztató.
5. Mentési dokumentáció: Ez a dokumentum az adatmentési folyamatokat és eljárásokat írja le, beleértve a mentési tervet, a mentési protokollokat és az adatok helyreállít
6. Információbiztonsági kézikönyv: Az információbiztonsági kézikönyv a szervezet informatikai biztonsági folyamatait és eljárásait részletesen tartalmazza, ideértve a hozzáférés-kezelést, az adatvédelmi eljárásokat és az incidenskezelést is.
7. Felhasználói szabályzat: A felhasználói szabályzat részletesen meghatározza azokat a szabályokat és eljárásokat, amelyeket az intézmény dolgozói kötelesek betartani, beleértve a jelszóhasználatot, az internetes használatot és az e-mail használatot is.
8. Biztonsági audit jelentések: A biztonsági audit jelentések dokumentálják az intézmény informatikai rendszerének ellenőrzését és értékelését. A jelentésekben szerepelnek azonosított hibák és javaslatok a rendszer javítására.
9. Rendszerbevezetési dokumentáció: A rendszerbevezetési dokumentáció leírja az informatikai rendszer telepítését és konfigurálását, valamint az alkalmazott biztonsági beállításokat és teszteket.
10. Rendszerfelügyeleti naplók: A rendszerfelügyeleti naplók naplózófájlok, amelyek a rendszerben végrehajtot
11. időegységre eső pénzösszeggel [Ft/év], vagy ha ez nem meghatározható, akkor „osztályzattal”, ami a kockázat nagyságrendjét és elviselhetőséget mutatja. A kockázat függ a káros események bekövetkezési valószínűségétől [1/év] és ezen események bekövetkezéséből származó és pénzben kifejezett kártól [Ft] is