INFORMATIKAI BIZTONSÁGI SZABÁLYZAT[1]

2025

[1] A szabályzatot megállapította a Szenátus a 2018. május 23. napi ülésén a 20/2018.(05.23.) számú határozatával. Utoljára módosította a Szenátus a 2025. november 25. napı ülésén a 48/2025.(11.25.) számú határozatával. A szabályzat 2025. november 26 napjától hatályos.

Tartalomjegyzék

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az Eötvös József Főiskola Informatikai Biztonsági Szabályzata (továbbiakban IBSZ) a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény és a minősített adat védelméről szóló 2009. évi CLV. törvény alapján készült.

1. Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed az Eötvös József Főiskola valamennyi közalkalmazottjára, illetve egyéb más jogviszonyban – különösen munkaviszonyban vagy megbízotti jogviszonyban –, valamint az Eötvös József Főiskolán hallgatói jogviszonyban álló személyre.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed a Főiskola tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra, az adathordozók tárolására, felhasználására.

3. Az IBSZ biztonsági fokozata

Intézményünk alap biztonsági fokozatba tartozik. (Szervezeti adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.)

Intézményünk általános informatikai feldolgozást végez.

4. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:

- Szervezeti és Működési Szabályzattal,
- Leltározási Szabályzattal,
- Selejtezési Szabályzatával,
- Belső Ellenőrzési Szabályzattal,
- Informatikai Szabályzattal,
- Adatvédelmi Belső Szabályzattal.

5. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

5.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

5.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő és elérhető jogi, szervezeti, programozási, műszaki intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

5.3. A védelem felelőse

A védelem felelőse a mindenkori informatikai referens, az egységvezetők és a rendszergazdák.

A jelen szabályzatban foglaltak jogszerű végrehajtásáról az intézmény Kancellárja és Rektora gondoskodik.

6. Adatvédelmi felelősök feladatai

a) Informatikai referens feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése, javaslatok tétele a rendszer szűk keresztmetszeteinek felszámolására.

b) Egységvezető feladatai:

- meghatározza a védett adatok körét a szabályzat alapján,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét, ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése, az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységét adminisztrálja.

c) Rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős az intézmény informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer önadminisztrációját,

d) Felhasználó feladatai:

- az általa használt eszközöket, alkalmazásokat egyedi jelszóval védi és gondoskodik róla, hogy ezen azonosítókhoz más ne férhessen hozzá.

6.1. Az informatikai referens ellenőri feladatai

- évente legalább egy alkalommal részletesen beszámol az intézmény Rektorának és Kancellárjának az IBSZ előírásainak betartásáról, rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

6.2. Az informatikai referens jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a rendszergazdák oktatás formájában biztosítják, erről nyilvántartást vezetnek.

Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

7.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként – a belső adatvédelmi szabályzattal összhangban - aktualizálni kell, az IBSZ folyamatos aktualizálása az informatikai referens feladata, egyeztetve a Kancellária vezetőjével a jogi változások terén.

7.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik. A minősítést a 3. pontban található definíciók alapján kell végezni.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a jogszabályok mindenkori előírásainak.

A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell.

A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a rendszergazdák a felelősek.

A titkot képező adatok védelmét, a feldolgozás - az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

8. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete különösen fontos, hogy megelőző intézkedések alapján a veszélyhelyzetek elháríthatók legyenek.

8.1. Környezeti infrastruktúra okozta ártalmak

Elemi csapás – vis major:

- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.

Környezeti kár:

- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).

Közüzemi szolgáltatásba bekövetkező zavarok:

- feszültségkimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

8.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző- és riasztóberendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

9.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

9.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

9.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

10. Az informatikai eszközök környezetének védelme

10.1. Vagyonvédelmi előírások

- a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni, a gépterembe való be- és kilépés rendjét szabályozni kell,
- a számítógép monitorát lehetőleg úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a főiskola alkalmazottjai, ill. a hallgatói jogviszonnyal rendelkező diákok használhatják,
- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.
- a szerverszobába való be- és kilépést szabályozni kell, a forgalomról naplót kell vezetni
- csak az illetékes dolgozók tartózkodhatnak a szerverszobában
- munkaidőn túl csak a szerverszobában csak engedéllyel lehet dolgozni

- a szerverterminálok monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el

10.2. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a gépteremre, szerverszobára vonatkozóan az intézmény Tűzvédelmi Szabályzata tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

Az intézmény géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.

Az intézmény géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűz- és munkavédelmi megbízott tudtával, ill. engedélyével szabad végezni.

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az egységvezetők feladata.)

11. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

11.1. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

11.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést az informatikusok végezik.

A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Számítógép és egyéb eszköz szétbontását csak informatikus végezheti el.

11.3. Az informatikai feldolgozás folyamatának védelme

11.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen, tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- lehetőség szerint olyan szoftvereket kell vásárolni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
    - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
    - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

  A szerverek rendszergazda jelszavát az informatikai referens kezeli.
- adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

11.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

11.3.3. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

11.3.4. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá intézményünk Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

11.3.5. Selejtezés, sokszorosítás, másolás

A selejtezést az intézmény Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata, valamint Iratkezelési szabályzata alapján kell lefolytatni.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

11.3.6. Leltározás

A szoftvereket és adathordozókat a Leltározási és Leltárkészítési Szabályzatban foglaltaknak megfelelően kell leltározni.

11.3.7. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.

A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.

A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználóknak – a rendszergazdák által kijelölt helyre (Office 365 felhasználói fiók helyi címtára) – kell készíteni. Az archiválásban az informatikusok segítséget nyújtanak.

Nem megengedett a rendszergazdák által kontrollálhatatlan alkalmazások számára dokumentumainknak hozzáférést biztosítani (pl. nem a szervezeti felhős szolgáltatások használata). Az adatbiztonság két legfőbb aspektusa:

- az adatok megőrzésére, reprodukálhatóságára vonatkozó elvárás
- személyes adatok védelmének biztosítása

A szervereken tárolt adatokról a mentést rendszeresen el kell végezni, az ehhez szükséges eszközöket biztosítani kell. A mentésért a rendszergazdák a felelősek.

11.4. Szoftver védelem

11.4.1. Rendszerszoftver védelem

Az üzemeltetésért felelős vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

11.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról/licenszekről a leltárfelelősöknek naprakész nyilvántartást kell vezetni az IBSZ 1. számú melléklet szerint.

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében intézményünknek az üzleti évről készített beszámolót legalább 8 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

A programok nyilvántartásáért és működőképes állapotban való tartásáért az egységvezetők a felelősek.

12. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

12.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftverekről biztonsági másolatot kell készíteni.

12.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokkal kapcsolatban körültekintően kell eljárni, vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső fel- használói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni csak az informatikai referens tudtával és engedélyével szabad.

13. Ellenőrzés

Az intézmény éves belső ellenőrzési tervében rögzíti az ellenőrzés módját.

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.

A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

14. Záró rendelkezések

A Szenátus a Szabályzatot a 48/2025.(11.25.) számú határozatával elfogadta. Az Informatikai Biztonsági Szabályzat 2025. november 26-án lép hatályba.

Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

Baja, 2025. november 25.

Dr. Szilágyiné dr. Szinger Ibolya
rektor

Dr. Paska Mihály
kancellár

1. sz. melléklet

Eötvös József Főiskola

SZOFTVERNYILVÁNTARTÁS

szoftver neve:.....

szoftver gyártója:.....

leltárszám:.....

szoftver verziószáma:.....

szoftver leírása:.....

szoftver azonosító sorszáma,szériaszáma:.....

szükséges hardver környezet:.....

szükséges operációs rendszer, szoftverkörnyezet:.....

licensz feltételei (kik, hányan, hány számítógépen, mettől, meddig használhatják):
.....

szoftver típusa (OEM, frissítés):.....

darabszám:.....

egyéb:.....

adatfelvétel időpontja, adatfelvevő aláírása: .....

1. sz. függelék

Eötvös József Főiskola Vírusvédelmi Szabályzata

1. Cél és hatály

A szabályzat célja a vállalat informatikai rendszereinek és adatai biztonságának megőrzése a kártékony szoftverek (vírusok, trójaiak, zsarolóprogramok, spyware) ellen. Hatálya kiterjed:

- Minden munkavállalóra és alvállalkozóra.
- A vállalat tulajdonában lévő vagy bérelt eszközökre (szerverek, munkaállomások, mobil eszközök).
- A vállalat hálózati infrastruktúrájára és felhőszolgáltatásaira.

2. Alapelvek

- **Megelőzés elsődlegessége**: A vírusfertőzések elkerülése érdekében minden eszközön naprakész vírusvédelmi megoldás használata kötelező.
- **Automatikus frissítés**: Vírusvédelmi szoftverek és operációs rendszerek automatikus frissítése engedélyezett és kötelező.
- **Felhasználói felelősség**: A felhasználók nem tilthatják le a védelmi rendszereket, és kötelesek jelenteni minden gyanús tevékenységet.

3. Védelmi intézkedések

3.1 Végpontvédelem

- Minden munkaállomáson és szerveren valós idejű vírusvédelem aktív.
- USB és külső adathordozók automatikus vizsgálata csatlakoztatáskor.

3.2 Hálózatvédelem

- Tűzfal használata.
- Hálózati forgalom szűrése ismert kártékony IP-címek és domain-ek ellen.
- VPN használata távoli hozzáféréshez.

3.3 E-mail és webvédelem

- E-mail mellékletek és linkek automatikus vizsgálata.
- Spam- és phishing-szűrők alkalmazása.
- Webszűrés a kártékony weboldalak blokkolására.

4. Tiltások

- Ismeretlen forrásból származó szoftverek telepítése tilos.
- Külső adathordozók használata csak előzetes ellenőrzés után.
- Jogosulatlan hozzáférés a vírusvédelmi beállításokhoz tilos.

5. Incidenskezelés

- Vírusfertőzés gyanúja esetén azonnali jelentés az informatikai osztálynak.
- Fertőzött eszköz izolálása a hálózatról.
- Rendszer helyreállítása biztonsági mentésekből.
- Incidens dokumentálása és elemzése a jövőbeni megelőzés érdekében.

6. Felülvizsgálat

- A szabályzatot évente felül kell vizsgálni, és szükség esetén frissíteni az aktuális fenyegetések és jogszabályok alapján.

2. sz. függelék

Eötvös József Főiskola IT Szolgáltatási Szabályzat

1. Bevezetés és cél

Az IT Szolgáltatási Szabályzat célja, hogy meghatározza az informatikai rendszerek, eszközök és szolgáltatások használatának szabályait, biztosítsa az üzleti folyamatok zavartalan működését, valamint az adatbiztonságot és jogszabályi megfelelést.

2. Hatály és alkalmazási terület

A szabályzat minden munkavállalóra, külsős partnerre és alvállalkozóra vonatkozik, akik hozzáférnek a vállalat informatikai rendszereihez, hálózatához vagy eszközeihez.

3. IT Szolgáltatások

- **Hálózati szolgáltatások**: Internet, belső hálózat, VPN.
- **Eszközök**: Munkaállomások, laptopok, mobil eszközök.
- **Szoftverek**: Operációs rendszerek, irodai alkalmazások, vállalati szoftverek.
- **Felhasználói támogatás**: Helpdesk, hibabejelentés, karbantartás.

4. Biztonsági előírások

- **Jelszókezelés**: Minimum 8 karakter, nagybetű, kisbetű, szám és speciális karakter.
- **Hozzáférési jogosultságok**: Csak munkakörhöz szükséges hozzáférések.
- **Adatvédelem**: GDPR és helyi adatvédelmi jogszabályok betartása.
- **Eszközök védelme**: Vírusvédelem, titkosítás, automatikus frissítések.

5. Incidenskezelés

- Hibabejelentés: telefonon vagy e-mailen keresztül.
- Válaszidők:
    - Kritikus hiba: 1 órán belül.
    - Normál hiba: 4 órán belül.
- Biztonsági incidensek azonnali jelentése az IT osztálynak.

6. Eszközhasználati szabályok

- Céges eszközök kizárólag munkavégzésre használhatók.
- Személyes eszközök (BYOD) csak engedéllyel és biztonsági feltételek mellett.
- Tiltott: Jogosulatlan szoftverek telepítése, illegális tartalom letöltése.

7. Frissítések és karbantartás

- Operációs rendszer és alkalmazások frissítése automatikusan vagy IT által.
- Hardver karbantartás ütemezetten, előre jelzett időpontban.

8. Jogkövetkezmények

A szabályzat megsértése fegyelmi eljárást vonhat maga után, súlyos esetben jogi következményekkel.

3. sz. függelék

Eötvös József Főiskola IT Kockázatkezelési Szabályzat

1. Cél és hatály

A szabályzat célja az informatikai rendszerek és szolgáltatások biztonságának fenntartása, a kockázatok azonosítása, értékelése és kezelése annak érdekében, hogy az intézmény megfeleljen a jogszabályi előírásoknak (pl. GDPR) és biztosítsa az üzleti folyamatok zavartalan működését.
Hatálya kiterjed minden munkatársra, hallgatóra és külső partnerre, akik hozzáférnek az intézmény informatikai rendszereihez.

2. Kockázatkezelés alapelvei

- **Megelőzés elve**: A kockázatokat lehetőség szerint előre azonosítani és csökkenteni.
- **Arányosság elve**: A kockázatkezelési intézkedéseknek arányban kell állniuk a kockázat súlyosságával.
- **Folyamatos felülvizsgálat**: Az IT rendszeres időközönként ellenőrzi és frissíti a kockázatkezelési intézkedéseket.

3. Kockázatok azonosítása

Az IT osztály az alábbi területeken vizsgálja a kockázatokat:

- **Adatbiztonság**: Jogosulatlan hozzáférés, adatvesztés, GDPR sérülés.
- **Rendszerbiztonság**: Szerverek, hálózatok, Microsoft 365 és Neptun szolgáltatások.
- **Eszközbiztonság**: Céges és saját eszközök használata.
- **Humán tényezők**: Hibás jelszókezelés, social engineering támadások.

4. Kockázatok értékelése

- **Valószínűség és hatás alapján**:
    - Alacsony: Minimális hatás, könnyen kezelhető.
    - Közepes: Jelentős hatás, de kontrollálható.
    - Magas: Kritikus hatás, azonnali intézkedést igényel.

5. Kockázatkezelési intézkedések

- **Technikai intézkedések**:
    - Rendszeres biztonsági frissítések (Microsoft 365, szerverek).
    - Vírusvédelem és tűzfalak.
    - Adatmentés és visszaállítási terv.

  Szervezeti intézkedések:
    - Jogosultságkezelési szabályzat betartása.

- Felhasználói oktatás (jelszókezelés, phishing felismerés).

- **Incidenskezelés**:
  - Kritikus incidensek azonnali zárolása.
  - Bejelentés telefonon vagy e-mailben az IT Helpdesknek.

6. Felülvizsgálat és jelentés

- Éves kockázatfelmérés és dokumentálás.
- Jelentés az intézmény vezetésének a kritikus kockázatokról és intézkedésekről.

7. Felelősség

- Az IT osztály felel a kockázatkezelési folyamat végrehajtásáért.
- A felhasználók felelősek a szabályok betartásáért (pl. jelszókezelés, adatvédelem).

4. sz. függelék

Eötvös József Főiskola Jogosultságkezelési Szabályzat

1. Cél és hatály

A szabályzat célja, hogy meghatározza az informatikai rendszerekhez és szolgáltatásokhoz való hozzáférési jogosultságok kezelésének elveit és folyamatát a főiskolán. A szabályzat vonatkozik minden munkatársra, oktatóra, hallgatóra és külső partnerre, akik hozzáférést kapnak az intézmény informatikai rendszereihez.

2. Alkalmazási terület

A szabályzat az alábbi rendszerekre és szolgáltatásokra terjed ki:

- Microsoft 365 (Teams, Outlook, OneDrive, stb.)
- Neptun tanulmányi rendszer
- Intézményi szerverek és belső alkalmazások
- Helpdesk és IT szolgáltatások

3. Jogosultságkezelés alapelvei

- **Szükségesség elve**: Jogosultságot csak a munkakör vagy tanulmányi feladat ellátásához szükséges mértékben adunk.
- **Időkorlátos hozzáférés**: Ideiglenes jogosultságokat meghatározott időre kell biztosítani.
- **Átláthatóság és nyomon követhetőség**: Minden jogosultság kiadása és módosítása dokumentált.

4. Jogosultságok kiadása és módosítása

- A jogosultságok kiadásáról **nem az IT dönt**, hanem az illetékes vezető vagy adminisztrátor.
- Az IT feladata:
    - Jogosultságok technikai beállítása a Microsoft 365 és Neptun rendszerekben.
    - Jogosultságok módosítása a jóváhagyott kérelem alapján.
- Jogosultság igénylése:
    - Írásban (e-mail) vagy hivatalos belső rendszerben.
    - Tartalmaznia kell: felhasználó neve, kért jogosultság, indoklás, jóváhagyó neve.

5. Jelszókezelés

- Minden felhasználó felelős saját jelszavának biztonságáért.
- IT kizárólag jelszó-visszaállítást végezhet Microsoft és Neptun rendszerekben.

- Jelszavaknak meg kell felelni a **GDPR és intézményi biztonsági előírásoknak** (minimum hossz, komplexitás).

6. Jogosultságok felülvizsgálata

- Évente egyszer kötelező felülvizsgálni a jogosultságokat.
- Inaktív felhasználók hozzáféréseit az IT törli a jóváhagyás után.

7. Incidenskezelés

- Jogosultsági problémák bejelentése: **telefonon vagy e-mailben** az Informatikai Osztálynak.
- Kritikus incidensek (pl. jogosulatlan hozzáférés) esetén azonnali zárolás és vizsgálat.

8. Felelősség és jogkövetkezmények

- Jogosulatlan hozzáférés vagy szabályszegés esetén fegyelmi eljárás indulhat.
- Az IT nem felel a felhasználó által okozott adatvesztésért, ha az a szabályzat megszegéséből ered.

EÖTVÖS JÓZSEF FŐISKOLA
6500 Baja, Szegedi út 2.
Tel: +36 79 524 624
info@ejf.hu
www ejf.hu

Katasztrófa Terv Informatikai Hálózathoz

Eötvös József Főiskola

1. Kockázatok és Fenyegetések Azonosítása

- Természeti katasztrófák (pl. árvíz, földrengés)
- Emberi hibák (konfigurációs hibák, véletlen adatvesztés)
- Kiberbiztonsági támadások (DDoS, adatlopás, zsarolóvírusok)
- Hardver- és szoftverhibák (szerver meghibásodás, tároló meghibásodás)

2. Alapvető Infrastruktúra

- **Ubiquiti hálózati eszközök** (switchek, hozzáférési pontok - AP-k): biztosítják a hálózati kapcsolatokat a főiskolán.
- **IPFire tűzfal**: Szűri és védi a belső hálózatot az internet felől érkező fenyegetések ellen.
- **Két szerver**: Egy elsődleges szerver és egy backup szerver, amely az épület másik oldalán helyezkedik el, VEEAM szoftverrel a biztonsági mentésekhez.

3. Katasztrófa Kezelési Csapat és Felelősségek

- **IT Adminisztrátorok/Rendszergazdák**:
  - Hálózati infrastruktúra helyreállítása és a felhasználók támogatása.
  - Szerverek helyreállítása és adatok visszaállítása.
  - Fenyegetések elemzése, megelőzési és helyreállítási intézkedések felügyelete.
  - Kommunikáció a személyzettel, diákokkal és hatóságokkal.

4. Katasztrófa Kezelési Protokollok

- **Értesítési Lánc**: A katasztrófa bekövetkezésekor értesíteni kell az IT adminisztrátorokat/ rendszergazdát.
- **Kárfelmérés**: Határozzák meg az érintett eszközöket (pl. Ubiquiti switchek, IPFire tűzfal, szerverek, számítógépek) és a kár súlyosságát.

- **Döntési Terv**: Helyreállítandó rendszerek prioritási listája;
    - Internetkapcsolat
    - Belső hálózati eszközök
    - Szerverek és backup rendszer.
    - Végpontok.

5. Katasztrófahelyzet Specifikus Helyreállítási Lépések

A) Hálózati Eszközök Helyreállítása

- **Ubiquiti Switchek és AP-k**: Szükség esetén cseréljék ki az érintett eszközöket, és töltsék fel a legutolsó mentett konfigurációs beállításokat.
- **IPFire Tűzfal**: Amennyiben a tűzfal hardveresen érintett, használjanak tartalék tűzfalat, és töltsék fel az utolsó mentett konfigurációt.

B) Szerverek Helyreállítása

- Elsőként ellenőrizni kell az elsődleges szerver állapotát. Ha nem helyreállítható, indítsák el a backup szerverre történő átállást.
- **Backup Szerver**: Az épület másik felében található, ezért a fizikai elkülönítése megvédi a teljes adatvesztéstől.
- **VEEAM Backup Helyreállítási Eljárások**: A VEEAM által létrehozott mentéseket futtassák le az adatok visszaállításához. Legyenek külön mentési pontok elérhetők legalább napi rendszerességgel.

C) Végpontok Helyreállítása

- Elsőként ellenőrizni kell az elsődleges szerver állapotát. Ha nem helyreállítható, el kell végezni a végpont cseréjét.
- Ha helyreállítható, elsőként adatvesztés nélkül kell elvégezni, ha ez nem lehetséges akkor adatvesztéssel a végpont teljes újra telepítését kell elvégezni.
- Hardveres hiba esetén hardver cserével végzendő el a helyreállítás.

6. Adatbiztonság és Visszaállítás

- **Mentési és Archiválási Stratégia**: A kritikus adatokat napi szinten mentsék a backup szerverre. A VEEAM konfigurálásával biztosítsanak heti teljes mentést és napi inkrementális mentést.
- **Mentés Tesztelése**: Rendszeresen teszteljék a visszaállítási folyamatot, hogy biztosítsák az adatok visszaállíthatóságát katasztrófa esetén.

EÖTVÖS JÓZSEF FŐISKOLA
6500 Baja, Szegedi út 2.
Tel: +36 79 524 624
info@ejf.hu
www.ejf.hu

EÖTVÖS JÓZSEF FŐISKOLA BAJA

7. Kommunikáció és Felhasználói Támogatás

- Katasztrófa esetén kommunikálják a helyzetet a személyzet és a diákok felé e-mailben, a főiskola weboldalán és a személyzet felé telefonon.
- Nyújtsanak támogatást a felhasználók számára, hogy azok zökkenőmentesen használhassák az újrahuzalozott vagy helyreállított szolgáltatásokat.

8. Folyamatos Karbantartás és Képzés

- **Rendszeres Frissítések**: Az Ubiquiti eszközöket, IPFire tűzfalat és a szervereket tartsák naprakészen.
- **Képzés és Tudatosság**: Rendszeresen képezzék az IT csapatot, és tartsanak gyakorlatokat a katasztrófa forgatókönyvek kezelésére.

Kelt Baja, 2024. 11.18.

Varga Patrik

dr. Paska Mihály

6. sz. függelék

Informatikai Stratégia Dokumentum

1. Bevezetés Az alábbi dokumentum az Eötvös József Főiskola informatikai stratégiáját tartalmazza, amely a jelenlegi infrastruktúra elemzésén és a jövőbeli fejlesztési célokon alapul. Az intézmény célja egy megbízható, biztonságos és korszerű informatikai környezet fenntartása és fejlesztése, amely támogatja az oktatási és adminisztratív folyamatokat.

2. Jelenlegi Informatikai Infrastruktúra

2.1 Szerverszobák és hálózati infrastruktúra Az intézmény informatikai infrastruktúrája két szerverszobára épül, amelyek biztosítják az egyetem rendszerének zavartalan működését:

- **Nagyobb szerverszoba:** Ez a központi szerverszoba, ahol az intézmény fő hálózati eszközei találhatók. Itt két szerver üzemel, amelyek a központi szolgáltatásokat látják el. A szerverszobában található továbbá több switch, amely a csillagtopológia központjaként működik, így biztosítva az egyes hálózati eszközök hatékony és gyors kapcsolódását. A tűzfal a hálózat védelmét biztosítja a külső és belső fenyegetésekkel szemben, míg az UPS (szünetmentes tápegység) a hálózat folyamatos működését garantálja áramkimaradások esetén. A főiskola internetkapcsolata ezen a ponton keresztül érkezik egy optikai kábel segítségével.
- **Kisebb szerverszoba:** Ebben a szerverszobában található egy backup szerver, amely a fő szerverek adatainak biztonsági mentését végzi. Emellett pár switch gondoskodik az itt található hálózati eszközök megfelelő működéséről.
- **Rendezők:** Az intézményben két rendezőszekrény található, amelyek mindegyike pár switchet tartalmaz. Ezek a rendezők segítenek az intézmény hálózati kábelezésének szervezésében és optimalizálásában, biztosítva az adatforgalom zökkenőmentes áramlását.

2.2 Használt Rendszerek Az intézmény különböző rendszereket alkalmaz az oktatás, az adminisztráció és az ügyvitel támogatására:

- **Neptun** – oktatási keretrendszer, amely a hallgatók és oktatók adminisztrációját kezeli. Segítségével a hallgatók tantárgyakat vehetnek fel, vizsgákra jelentkezhetnek, valamint elérhetik tanulmányi eredményeiket.
- **Moodle** – egy nyílt forráskódú online oktatási rendszer, amely támogatja az e-learning alapú képzéseket. Lehetővé teszi kurzusok létrehozását, online vizsgák lebonyolítását és tananyagok megosztását.
- **FIR** – a felsőoktatási információs rendszer részeként az intézmény adatszolgáltatását biztosítja az oktatási hatóságok felé.
- **Gólya** – a felsőoktatási felvételi rendszer, amely lehetővé teszi a hallgatók felvételi eljárásának kezelését, nyomon követését.
- **TÜSZ** – teljes körű ügyviteli szolgáltató rendszer, amely az intézmény működéséhez szükséges adminisztratív feladatokat látja el, például pénzügyi és gazdálkodási folyamatokat.

- **KIRA** – bérügyviteli rendszer, amely az oktatók és alkalmazottak bérszámfejtését végzi.
- **Poszeidon** – elektronikus iktató rendszer, amely a hivatalos dokumentumok kezelését és archiválását biztosítja.
- **Drupal** – egy nyílt forráskódú tartalomkezelő rendszer, amely az intézmény weboldalának alapját képezi.

3. Fejlesztési Programok A főiskola informatikai fejlesztési stratégiája több programra épül, amelyek célja az infrastruktúra megbízhatóságának és teljesítményének növelése.

3.1 Alapinfrastruktúra fejlesztése Az intézmény célja, hogy informatikai infrastruktúráját folyamatosan fejlessze és korszerűsítse. Ennek érdekében:

- A meglévő szervereket és hálózati eszközöket folyamatosan modernizálják, új hardverek beszerzésével és a régi eszközök cseréjével.
- A szerverek redundanciáját növelik, hogy biztosítsák az adatok és szolgáltatások folyamatos elérhetőségét.
- A redundancia növelése érdekében további szerverek és backup megoldások kerülnek bevezetésre.
- A hálózati infrastruktúrát korszerűsítik, új optikai kapcsolatokkal és megnövelt sávszélességgel.
- A hálózati kábelezést rendszeresen ellenőrzik, és szükség szerint frissítik az új szabványoknak megfelelően
- A biztonsági intézkedéseket fejlesztik, például fejlettebb tűzfalmegoldásokkal és behatolásérzékelő rendszerekkel.

3.2 Adatátviteli hálózat fejlesztése

- Az optikai kapcsolat kapacitásának növelése révén gyorsabb és stabilabb adatátvitelt érnek el.
- Minőségi szolgáltatás (QoS) bevezetése az egyes adatfolyamok prioritizálására.
- Új hálózati szegmensek kialakítása az új épületek számára

3.3 Hálózati aktív eszközök fejlesztése

- Új generációs switch-ek telepítése, amelyek támogatják a 10G kapcsolatokat.
- Nagyobb kapacitású és jobb lefedettséget biztosító Wi-Fi hálózat kiépítése.

3.4 Alapszolgáltatások fejlesztése

- Dokumentumkezelő rendszer modernizálása a könnyebb kereshetőség és hozzáférés érdekében.
- Online ügyfélszolgálati rendszer fejlesztése a hallgatói és oktatói kérések hatékonyabb kezelése érdekében.

3.5 Szerverkonszolidációs program

- A meglévő **Hyper-V** alapú virtualizációs környezet bővítése, teljesítményének növelése.
- További redundáns szerverek beállítása a megbízhatóság fokozása érdekében.
- Az adatmentési és visszaállítási rendszerek fejlesztése.

3.6 UPS és Klíma karbantartás

- Rendszeres karbantartási ütemterv kidolgozása.
- Új generációs UPS-ek és energiatakarékos hűtőrendszerek bevezetése.

3.7 Új épület informatikai infrastruktúra

- Modern hálózati infrastruktúra kiépítése az új oktatási és kutatási helyszíneken.
- Teljes körű hálózati kábelezés.
- Modern AP-k telepítése Wi-Fi lefedettség növelésére.
- Új szerverszoba kialakítása

4. Kockázatok és Kihívások

- Rendszerbiztonság fenntartása.
- Kibertámadások elleni védekezés erősítése.
- Finanszírozási források biztosítása.

5. Összegzés A fejlesztési programok biztosítják, hogy az intézmény informatikai rendszere korszerű, biztonságos és jövőálló maradjon.