ESZTERGOMI
SZAKKÉPZÉSI
CENTRUM

Az Esztergomi Szakképzési Centrum Informatikai Biztonsági Szabályzata

Készítette:

.....
Simon Attila
gazdasági vezető

Jóváhagyta:

.....
Kovács Tamás
kancellár

Esztergom, 2025. 01.31.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

1. Az Informatikai Biztonsági Szabályzat (IBSZ) célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem 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,
- az adatfeldolgozás 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 üzembehelyezésen keresztül az üzemeltetésig.
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 adott intézményre és annak szervezeti egységeire.

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 szervezet tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

Az intézmény adatai különböző biztonsági fokozatba tartozhatnak. (hivatali 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 adatok)

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:
- Az intézmény belső szabályzataival
- Számviteli politikával

6. 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.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- 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,

6.2. A védelem eszközei

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

7. A védelem felelőse

A védelem felelőse a mindenkori informatikai vezető/rendszergazda.
A jelen szabályzatban foglaltak szakszerű végrehajtatásáról az intézmény vezetőjének (kancellárjának) kell gondoskodnia.

7.1. Adatvédelmi felelősök feladatai

a) Informatikai vezető/rendszergazda feladatai:
– az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
– javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
– meghatározza a védett adatok körét,
– ellátja az adatkezelés és adatfeldolgozás felügyeletét,
– ellenőrzi a védelmi előírások betartását,
– az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
– az adatvédelmi feladatok ismertetése,
– ellenőri tevékenységét adminisztrálja.
– ellenőrzi a szoftverek használatának jogszerűségét

b) 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 a vállalkozás informatikai rendszer hardver eszközeinek karbantartásáért,
– nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
– gondoskodik a folyamatos vírusvédelemről
– a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
– folyamatosan figyelemmel kíséri és vizsgálja a rendszer működését és biztonságát,
– ellenőrzi a rendszer adminisztrációját,

7.2. Az intézményvezető (kancellár) ellenőri feladatai

– évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
– rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
– előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

7.3. Az intézményvezető (kancellár) ellenőri feladatainak teljesítéséhez kapcsolódó jogai

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

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére megismerési nyilatkozat alapján köteles biztosítani a Centrum.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. Az informatikai eszközök használatának szabályozása

8.1.1
A munkáltató informatikai rendszerének védelmének érdekében a Munkáltató írásos hozzájárulása hiányában a Munkavállaló a Munkáltató által biztosított internet hozzáférést, postafiókot és számítógépet (a továbbiakban munkáltatói informatikai eszközök) kizárólag munkavégzés céljára jogosult használni.

8.1.2.
A munkavállaló kötelezettsége, hogy munkakörével kapcsolatban nem használ fel nem legális szoftvertermékét és munkáltatói informatikai eszközökön nem tart és nem futtat nem legális szoftvertermékeket

8.1.3
A munkavállaló a munkaviszonyával összefüggésben használatra kapott programokat, adatállományokat és egyéb szoftvertermékeket kizárólag a munkáltatói informatikai eszközökön tárolhatja és futtathatja, azokról a munkáltató kifejezett írásbeli engedélye nélkül másolatot nem készíthet

8.1.4
A munkáltató informatikai rendszerének védelme érdekében, az ESZC jogosult a munkáltatói informatikai eszközökre szoftveres védelmi eszközöket telepíteni és jogosult a munkáltatói informatikai eszközök ellenőrzésére, különösen a munkavállaló által látogatott honlapok kilistázására, és az elektronikus postafiókba érkezett vagy onnan küldött elektronikus levelek fejlécének megtekintésére. A munkáltató a hivatalos tárgyú beérkező és kimenő elektronikus levelekbe jogosult betekinteni és azokazt archiválni.

8.1.5
Az a munkavállaló, aki az informatikai ellenőrzést nem teszi lehetővé, úgy tekintendő, mint aki a 8.1.1.8.1.4 pontban foglalt informatikai kötelezettségeit megszegte

8.2 Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél és annak szervezeti egységeinél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az informatikai vezető feladata.

8.3. 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.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi 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, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének jelenteni kell.
Iskolai informatikusról van szó akkor azt a szakmai felettesének kell, hogy jelezze.
A Centrum rendszergazdája pedig a Kancellárnak és az Adatvédelmi felelősnek kell, hogy jelezze.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető/rendszergazda a felelős.

Az 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).

9. Az informatikai eszközbázist veszélyeztető helyzetek

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

9.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
- 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:
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

9.2. 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 riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

10.1. Tervezés és előkészítés során előforduló veszélyforrások

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

10.2. A rendszerek megvalósítása során előforduló veszélyforrások

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

10.3. A működés és fejlesztés során előforduló veszélyforrások

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

11. Az informatikai eszközök környezetének védelme

11.1. Vagyonvédelmi előírások

– a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
– a gépterembe való be- és kilépés rendjét szabályozni kell,
– a gépterembe, szerverterembe történő illetéktelen behatolás tényét a szervezet vezetőjének azonnal jelenteni kell,
– az informatikai eszközöket csak a szervezet arra felhatalmazott alkalmazottai használhatják,
– az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

11.2. Adathordozók

– könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
– az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
– a használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
– a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
– adathordozót másnak átadni csak engedéllyel szabad,
– a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.3. Tűzvédelem

A gépterem, illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
Az intézmény géptermeibe, szerverszobáiba, vagy azok közvetlen közelébe minimum 1-1 db tűzoltó készüléket kell elhelyezni
Az intézmény géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető 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 informatikai vezető/rendszergazda feladata.)

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. 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.

12.2. 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 végzik.
A munkák szervezésénél figyelembe kell venni:
– a gyártó előírásait, ajánlatait,
– a tapasztalatokat.
Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. 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,
– az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a 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 személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető/rendszergazda kezeli.
  Az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

12.3.2. 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.

12.3.3. Adathordozók tárolása

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

12.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

12.3.6. Selejtezés, sokszorosítás, másolás

A selejtezést a vállalkozás selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

12.3.8. Leltározás

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

12.3.9. 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 felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazdák a felelősek.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver (operációs rendszer) védelem

A rendszergazdáknak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

12.4.2. 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 a leltárfelelősöknek naprakész nyilvántartást kell vezetni
A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a vállalkozásoknak az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 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 a vezetők a felelősek.

13. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

13.1. Kiszolgáló gépek

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

13.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A vállalkozás informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói 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 eszköz leltárfelelőse tudtával és engedélyével szabad.

14. Ellenőrzés

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.

15. Beléptetőrendszer

Az intézményekbe történő ki- és belépés szabályai

Az intézményekbe történő be- és kijutás elektronikus beléptető-rendszeren keresztül, ***belépőkártyával*** történik. Az intézmény területén jogszerűen csak belépőkártyával szabad tartózkodni.

a) A belépőkártya használata

A belépőkártya személy azonosítására alkalmas, tartalmazza a felhasználó nevét, oktatási azonosítóját.

A Belépőkártya nem átruházható, másnak használatra átadni tilos.

A beléptető kártyát a tanuló az osztályfőnöktől veheti át; a tanulói jogviszony megszűnésekor az iskolatitkárnál köteles azt leadni.

Ha a tanuló otthon felejti a beléptető kártyát, az iskola portáján ***pótkártyát*** kell felvennie. A pótkártya az intézményből nem vihető ki, kilépésre nem alkalmas. A pótkártya használóját a

portás lépteti ki. A pótkártyát a tanítási nap végén a portán kell leadni, A pótkártya használatának idejére a tanuló eredeti kártyája nem használható (letiltott).

b) Az iskola elhagyásának szabályai

A tanuló szabályosan a külső helyszínen tartott foglalkozásokra, illetve az órarendje szerinti tanítási idő után (órarend alapú kiléptetés), minden esetben a belépőkártya használatával hagyhatja el az iskolát.

A be- és kilépés adatai (időpontját) elektronikus rendszer rögzíti és 45 napig tárolja.

A tanítási idő vége előtt a tanuló csak külön, írásbeli engedéllyel léphet ki az iskolából. ki. Az engedélyt az iskola portásának kell leadni, aki az ***órarend alapú kiléptetést*** felfüggeszti. A tanuló ezt követően tud a kártya használatával kilépni.

A csoportos kilépés a kísérő tanárral, a kísérő tanár kártyájával történik. A csoportos kilépés idejére a portás az órarend alapú kiléptetést felfüggeszti.

Épület – pl. tűzriadó miatti – kiürítése esetén a portáról vezérelhető vésznyitóval nyitható a kapu és ejthető le a beléptető rendszer forgóvillája. Vész- ill. katasztrófahelyzet esetén a falon elhelyezett vésznyitó is használható.

c) Vendégek (szülők/törvényes képviselők, jogviszonnyal nem rendelkező egyéb személyek) beléptetése

Az iskola hivatalos programjaira érkező vendégek beléptetése – a vendégek regisztrálása mellett – a portás által kezelt vendégkártyával történik.

A be nem jelentett, előre nem egyeztetett időpontra (spontán) érkező személyek beléptetése igazgatói engedély alapján történhet. Ilyen esetekben a portásnak nincs jogosultsága a belépést önállóan engedélyezni.

d) Adatkezelési tájékoztató

A beléptetőrendszerrel kapcsolatos, részletes adatkezelési tájékoztató az intézmény weboldalán érhető el.

A beléptetőrendszerrel kapcsolatos adatkezelési eljárásrendet az intézmény weboldalán és az eszc.eu weboldalon elérhető *„Adatkezelési és Adatvédelmi Szabályzat"* tartalmazza.

16. Záró rendelkezések

Az Informatikai Biztonsági Szabályzat 2025 02.01-jén lép hatályba.
Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.