INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályba lépés dátuma: 2018. március 1.

IV. Sz. Gazdasági Működtető Központ
1.
Győr

Papp Lászlóné
Igazgató

Tartalomjegyzék:

Informatikai Biztonsági Szabályzat

A IV. sz. Gazdasági Működtető Központ alá tartozó (továbbiakban: IV. sz. G.M.K. vagy „intézmények") Informatikai Biztonsági Szabályzatát, (továbbiakban: IBSZ) a következők szerint határoztam meg az intézmény valamennyi telephelyére vonatkozóan:

Az Informatikai Biztonsági Szabályzat az alábbi jogszabályokon alapul:

- Az állami és önkormányzati szervek elektronikus információ biztonságáról szóló 2013. évi L. törvény
- A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény

Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatikai alkalmazása során biztosítsa az Intézményben az alábbiakat:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását
- az üzemeltett számítógépek, informatikai eszközök, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát
- az üzembiztonságot szolgáló karbantartást és fenntartást
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre csökkentését
- az adatállományok tartalmi és formai épségének megőrzését
- munkaállomásokon lekérdezhető adatok körének meghatározását
- adatállományok biztonságos mentését
- a számítógépes rendszerek zavartalan üzemeltetését
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását
- az adatvédelem és adatbiztonság feltételeit
- a védelem működését a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen IBSZ az intézmény adatvédelmének általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét. Szabályozza a számítástechnikai, informatikai eszközök használatának adatvédelmi biztonsági szabályait.

Műszaki alapfogalmak

Szerver

Olyan hálózatra kapcsolt, központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza.

Munkaállomás

Egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál.

Iroda

Az a légkondicionált/nem légkondicionált helyiség, ahol az intézményi dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz, használhatják az IBSZ-ben meghatározottak szerint.

Szerver terem

Az a légkondicionált, biztonsági berendezésekkel ellátott helyiség, ahol a szerverek vannak, és csak a rendszergazda tevékenykedhet felelősségteljesen. Más személy ott tartózkodása csak a rendszergazda engedélyével történhet!

Rack szekrény:

Üvegezett, biztonságos fém szekrény, amelyben hálózati eszközöket, szervereket, telefon és más adatkapcsolati rendszereknek helyet adó speciális szekrény.

Adat

A számítástechnikában nevezzük a számokkal leírható dolgokat, melyek számítástechnikai eszközökkel rögzíthetők, feldolgozhatóak, és megjeleníthetők. Adatnak minősül minden

olyan digitális és nyomtatott információ ami az IV. sz. GMK munkakörnyezetében képződik és tárol, beleértve az alárendelt intézmény hálózatokat is.

Adatállomány

Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz

Adatbiztonság

Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere

Adatfeldolgozás

Az adatok gyűjtése, rendszerezése, törlése, archiválása

Adatvédelem

Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik

Alkalmazói program (alkalmazói szoftver)

Olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja

Felhasználó

Az a személy vagy szervezet, aki (amely) egy vagy több informatikai rendszert használ munkavégzése folyamán, feladatai megoldásához.

Hardver

Az informatikai rendszer eszközeit, fizikai elemeit alkotó részei

Hálózat

Két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé

Informatikai biztonság

Olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni

Rendszerprogram (rendszer szoftver)

Olyan alapszoftver, amelyre szükség van, hogy valamely rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

A Szabályzat hatálya

Az IBSZ hatálya kiterjed az alábbi intézményekre:

1. IV. sz. Gazdasági Működtető Központra és dolgozóira
2. EBI Egyesített Bölcsődei Intézmény hálózatra és dolgozóira
3. Győr Megyei jogú város Gyermektáborra és dolgozóira
4. IV. Sz. Gazdasági Működtető Központ működtetésében lévő óvodákra és dolgozóira

Az IBSZ területi, személyi és tárgyi hatálya az intézményrendszerek valamennyi dolgozójára érvényes.

Tárgyi hatálya kiterjed:

- A védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül
- Az adatok felhasználására, tárolására vonatkozó utasításokra
- Az adathordozók tárolására, felhasználására
- Az intézmény tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációira is
- A számítástechnikai folyamatban szereplő összes dokumentációra is (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció)
- A rendszer és felhasználói programokra

Kapcsolódó szabályozások

Az IBSZ- az Intézmény Szervezeti és Működési Szabályzatával és mellékleteivel, továbbá az adatvédelmi és adatbiztonsági szabályzattal összhangban kell alkalmazni.

Védelmet igénylő adatok, eszközök köre

A védelem tárgya

- Az alkalmazott hardver eszközök és azok működési biztonsága
- A számítástechnikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk
- Az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig
- Az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer-szoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága
- Személyhez fűződő és vagyoni jogok
- Az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai

A védelem eszközei

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

A kiemelt védelem felelőse

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény rendszergazdájának kell gondoskodnia. / továbbiakban adatvédelmi felelős /

Az adatvédelmi felelős feladatai, dolgozói, felhasználói személyeknél

- Ellátja az adatfeldolgozás számítástechnikai felügyeletét
- Ellenőrzi a védelmi előírások betartatását
- Ellátja a számítástechnikai titokvédelmi munka szervezését és felügyeletét

- A védelmi eszközök alkalmazására vonatkozó döntés előkészítése érdekében a szakterületek bevonásával biztonságot növelő intézkedések kialakítása
- Felügyeli a számítástechnikai rendszerek üzembiztonságát, biztonsági másolatok, adatmentések készítését hálózatra
- A védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos felügyelete
- Adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása
- Adatvédelmi feladatok ismertetése
- A védelmi rendszer érvényesülésének felügyelete
- Az IBSZ kezelése, naprakészen tartása, módosítások átvezetése javaslatot tesz
- Ellenőrzi a vírusvédelem meglétét és használatát, frissítését
- Redkívüli dolgokról egyeztet az intézmény vezetőjével.

Az adatvédelmi felelős feladatai / rendszergazda /

- Évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását
- Rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot
- Ellenőrzi a számítástechnikai munkafolyamatok részét
- Adatvédelmi szempontból, ellenőrzi az IBSZ naprakészségét, illetve azok végrehajtását

Az adatvédelmi felelős jogai

- Az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézményvezetőnél
- Bármely érintett szervezeti egységnél jogosult informatikai eszközök szakszerű használatának ellenőrzésre
- Javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére
- Adatvédelmi szempontból a felhasználókat oktatja

Az intézményi informatikus feladatai

Az informatikus feladatait a munkaköri leírása szerint látja el.

A felhasználó kötelessége:

- Informatikai tudásának folyamatos fejlesztése
- Tájékozott a munkavégzésre átadott technikai eszközök használatában
- Elsajátítja a munkájához szükséges informatikai tudást
- A rábízott adatokat és információkat bizalmasan kezeli
- A tudomására jutott szabálytalan dolgokat haladéktalanul jelenti vezetőjének
- Adathordozókat, adatátviteli eszközöket nem csatlakoztathat intézményi géphálózathoz, intézmény területére nem hozhatja be.
- E-mail és web forgalmat csak céges ügyben használhatja
- külső eszközt nem csatlakoztat a belső hálózatra
- Rá bízott jelszavakat megőrzi, gépét jelszavas védelemmel védi
- E-mail címet nem regisztrálhat /rendszergazdai engedély szükséges /
- Sem informatikai, sem egyéb technikai információt nem adhat át külsösnek
- Rábízott eszközöket megóvja, tisztán tartja, rendeltetésszerűen használja
- Önállóan képzi magát, hogy a rendelkezésére bocsájtott IT eszközöket magas színvonalon tudja használni

Kiemelt adatvédelmi feladatok:

- A védelmi rendszer érvényesülésének biztosítása
- Biztosítja a számítástechnikai eszközök védelmét a szervezeti egységek számára
- A központi szervezeti egység és a IV. sz. GMK, és a IV. GMK-val munkamegosztási megállapodás alapján együttműködő intézmények számítógépes rendszerének szakszerű használata és az ehhez kapcsolódó számítástechnikai, adatvédelmi szolgáltatások betartása.

Az IBSZ alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére az intézmény vezető biztosítja, az egyes munkaköri leírásoknak és az IBSZ előírásainak megfelelően.

Az IBSZ karbantartása

Az IBSZ-t a számítástechnikában, informatikában, valamint az intézményben bekövetkező változások miatt időközönként aktualizálni kell. Ez az adatvédelmi felelős feladata.

A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság
Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

1. közlésre szánt (bárki által megismerhető) adatok
2. minősített adatok (titoknak minősülnek)

- A számítógépes feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme hatáskörébe tartozik.
- Az intézményi titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.
- A kijelölt dolgozók előtt a titokvédelmi és egyéb rendszabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

A titkot képező adatok védelmét, a feldolgozás – adattovábbítás, tárolás – során az operációs rendszerben és a felhasználói programban alkalmazott titkosítással, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftveres és hardveres adatvédelem).

Szervezeti egységek védelmi eszközei és módszerei

A szervezeti egység vezetője önállóan dönt a védelmi eszközökről, szemelőt tartva az intézmény informatikai struktúrájának megfelelő biztosítását.

Tűzvédelem

A gépterem, illetve kiszolgáló helyisége és a (szerverterem) a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a gépterem (számítógépes szoba) szerverterem „Tűzvédelmi utasítás" – a tartalmazza, amely az intézmény tűzvédelmi szabályzatának részét képezi.

Vagyonvédelem, fizikai biztonság

- a géptermeket biztonsági zárakkal kell felszerelni
- a gépterembe való be- és kilépés rendjét szabályozni kell
- a gépterem kulcsának felvétele és leadása csak aláírás ellenében a személyazonosság igazolása mellet történhet
- munkaidőben és azon túl a gépteremben csak engedéllyel lehet tartózkodni, kivétel a rendszergazda
- a gépterembe történő illetéktelen behatolás tényét a szervezet vezetőjének azonnal jelenteni kell
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt dolgozók használhatják
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős
- az intézményi hálózatra idegen PC, telefon, tablet, egyéb digitális eszköz nem csatlakoztatható

Adathordozók védelme, tárolása, hordozása és karbantartása

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolása közben ne sérüljenek, károsodjanak
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni
- a nyilvántartásban az azonosító adaton kívül a felírás és megőrzés dátumát, a védettség tényét, a jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni
- a használni kívánt adathordozót (floppy disk, pendrive, CD-ROM, HDD stb.) a tárolásra kijelölt helyről kell kivenni és oda kell vissza is helyezni
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet
- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek

- adathordozót más intézménynek átadni csak a rendszergazda engedélyével lehet
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg
- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell

Selejtezendő:

- a fizikailag sérült, javítása gazdaságtalan, javíthatatlan
- a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott)
- szakvélemény alapján elavult eszköz
- ha a kapacitási hibák jelentkeznek
- véglegesen elhasználódott adathordozót

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni, bizalmas adatokat, felhasználói és rendszerprogramokat tartalmaz adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag megsemmisíteni az adathordozót.
A selejtezést a Selejtezési Szabályzatnak és az Intézményi Iratkezelési Szabályzatának megfelelően kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni, az üzemi másolás nem minősül másolásnak, biztonsági, illetve archív adatállomány előállítása másolásnak számít.
Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

Adatvédelmi feladatok

- az adatátvitel hibátlan műszaki állapotú berendezésen történjen
- csak tesztelt adathordozóra lehet adatállományt rögzíteni
- adatrögzítés szoftver védelme: a programokat és az adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és 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

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adattárolókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

Vírusvédelem

A munkaállomásokon és szervereken, vírusvédelmi rendszert kell kialakítani. Vírusellenőrzést és vírusirtást kell végrehajtani ha a rendszer gazdája azt szükségesnek ítéli meg. Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben erre nincs lehetőség (pl. munkaidőn kívül) a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes rendszergazda, informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a szervezeti egység vezetőjének ki kel deríteni a fertőzés lehetséges okait, a szükséges védelmi intézkedést meg kell hoznia.

Szoftver védelem

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

Rendszerszoftver védelem

- A rendszerszoftver módosításához az illetékes engedélye szükséges
- A módosítással egy időben, a dokumentációban is át kell a változtatásokat vezetni
- A rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni (eseménynapló)

Programokhoz való hozzáférés, wifi, PC védelem, programvédelem

A PC eszközöket minden esetben jelszavas védelemmel kell ellátni! WIFI hálózatoknak az intézményi felhasználása csak olyan eszköz engedélyezett amely az intézmény

tulajdonát képezi. Ezek az eszközök jogosultak a hálózat használatára. Új eszköz beléptetése csak rendszergazdai engedéllyel lehetséges, rendszergazda jelenlétében. Rendszerek jelszavas védelmét a rendszergazda kezeli!

A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációit.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója
- a program készítőjének neve
- a feldolgozási rendszer megnevezése

Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni
- a nyilvántartásból egyértelműen megállapíthatóak legyenek a program azonosítására és kezelésére vonatkozó adatok

Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni

Hardver védelem

- a számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől
- számítógép közelében ételt és italt fogyasztani tilos
- a számítógépteremben és a szerver teremben klímaberendezés használata ajánlott
- szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerver-teremben kell elhelyezni
- a számítógép-hálózat csatornáit külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát
- a fali csatlakozók megbontása szigorúan tilos

- csak földelt aljatokat lehet használni számítógép üzemeltetéséhez
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak (alapelv: sűrűn használt utat szabadon kell hagyni)
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes rendszergazda, illetve a szervizek szakemberei nyúlhatnak bele
- havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni

Az intézmény további védelmi előírásai

A védelem felelőse az intézményvezető.

Védelmi előírások

- a számítógépeket csak indítójelszóval lehessen elindítani
- szerverek megfelelő bonyolultságú jelszavas védelemmel védi
- induláskor minden esetben vírus-ellenőrző programot kell elindítani
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell
- új eszközök beszerzésénél csak a rendszergazda által ellenőrzött gépek kerülhetnek az intézményi hálózatba
- rendszer jelszavakkal a rendszergazda rendelkezik, csak írásos igény esetén adható ki, rendszerátadás céljából
- jelszót szóban, telefonon, sms-ben, chat rendszeren történő átadása, TILOS!
- minkét esetben a jelszóknak különbözőknek kell lenniük
- a bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel vagy külső programmal is
- a módosításokról napi mentést kell készíteni, ezeket a havi mentésekig kell megőrizni
- a teljes anyagról heti mentéseket kell készíteni, ezeket a havi mentésekig meghatározott ideig kell megőrizni
- a felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól külön, tűzbiztos helyen kell tárolni.

Szerverszoba / gépterem / rendje

1. A számítógépteremben/szerverszoba helyiségben a rendszergazdán kívül más nem tartózkodhat. Más személyek benntartózkodását a rendszergazda engedélyezheti.
2. Üzemidőn kívül az ajtót zárva kell tartani és a kulcsokat le kell adni. A gépterem kulcsát csak az rendszergazda felelős által összeállított külön listán szereplő személyek kaphatják meg. Munkaidőn belül és kívül idegen személy csak rendszergazdai felügyelet mellett tartózkodhat a gépteremben. A géptermet áramtalanítani csak a rendszergazda engedélyével lehet.
3. A gépteremben az esztétikus, higiénikus, folyamatos munkavégzés feltételeit kell megőrizni. A géptermi rend megtartásáért és a biztonságos műszaki üzemeltetésért a kijelölt rendszergazda a felelős.
4. A gépterembe ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!
5. A gépterembe égő cigarettával belépni, és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!
6. A gépterem takarítását csak az arra előzőleg kioktatott személyek végezhetik.
7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a gépterem kezelője és a szervizek szakemberei végezhetnek.
8. A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani.
9. A gépteremben elhelyezett adathordozókat csak a rendszergazda engedélyével lehet használni.
10. Adathordozókat, leporellót csak a rendszergazda engedélyével lehet be- és kivinni a gépteremből.
11. Az elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet.
12. A gépteremben elhelyezett jelzőberendezések (klíma, tűz- és betörésjelző) műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak és bármilyen rendellenességet azonnal jelenteni kell a működésükért felelős megbízottaknak.
13. A gépteremben idegen jelenléte esetén csak rendszergazdával tartózkodhat

14. A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

Az intézményeknél alkalmazott számítógépes rendszerek

A rendszer pontos megnevezése	A bevezetés időpontja	A rendszer használatára felhatalmazott személyek	
		neve	aláírása
Win SRV. 2012-16	2012.10	Bazsó Ádám	Bazsó Ádám
V.M. XP prof.	2012.10	Bazsó Ádám	Bazsó Ádám
Wiebed	2012.10	Felhasználók	
Thinstuff	2012.10	Bazsó Ádám	
XP, Win7-10 Kliens	2012.10	Felhasználók	
Wimenza	2016.01	Felhasználók	
Office 2008-2016	2012.10	Felhasználók	
Bölcsi rendszer	2017.07	Bazsó Ádám	Bazsó Ádám

Hatályba lépés

Ezen szabályzat 2018. március 1-én lép hatályba, és ezzel egyidejűleg a 2017. július 1-én kiadott Informatikai Biztonsági szabályzat és számítógép-használati szabályzat hatályát veszti.

EGYESÜLT BÖLCSŐDEI
2023 Győr, Kodály Z. u. 18.

A jelen Szabályzat előírásait a ..... vonatkozóan átveszi, és azt saját szabályzatként kiadja 2018. március 1-jei hatállyal.

Győr, 2018. március 1.

.....

~~óvodavezető~~/igazgató

Megismerési, legitimációs záradék

2018. 03. 01.-én a GMK **Informatikai biztonsági szabályzatát és számítógéphasználati szabályzatát** megismertem

Intézmény	Név	Aláírás
GMK Gazdasági Hivatal	Papp Lászlóné igazgató	
	Matisné Kertész Judit gazdasági vezető	
	Árbik Noémi	
	Baksáné Szollár Petronella	
	Bárányné Tóth Beáta	
	Bazsó Ádám	
	Bendes Eszter	
	Bondor Orsolya	
	Csikós Henriett	
	Csudainé Fodor Tünde	
	Grichisch Jánosné	
	Hécz Viktória	
	Horváthné Mészáros Brigitta	
	Ivánkai Dániel	
	Kalmárné Nagy Márta	
	Kőművesné Kertész Eszter	
	Menyhárt Ádám	
	Molnárné Munkácsy Magdolna	
	Némethné Lőkös Enikő	
	Péczy Szabina	
	Pozsgai Pálné	
	Szilágyi Lászlóné	
	Szollár Sándorné	
	Tanyás Csabáné	
	Tornyos Andrea	
	Tóth Krisztina	
	Tóth Lívia	