Szombathelyi Köznevelési GAMESZ

Székhely: Szombathely, Nádasdy Ferenc u.4.
Telephely: Szombathely, Boglárka u.2.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Érvényes: 2023. 01. 01-től

Szombathelyi Köznevelési GAMESZ 9700 Szombathely, Nádasdy F. u. 4. 1

Jóváhagyta: .....

Imréné Erényi Katalin
Igazgató

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A Szombathelyi Köznevelési GAMESZ (székhely: 9700 Szombathely, Nádasdy 4., Törzskönyvi azonosító szám: 421151, adószám: 15421151-2-18) továbbiakban, mint Adatkezelő a jelen Informatikai Biztonsági Szabályzat keretei között (IBSZ) rögzíti az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR, továbbiakban: GDPR vagy Rendelet) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) rendelkezéseinek végrehajtása érdekében az adatvédelemmel kapcsolatos irányadó szabályokat, az ezzel kapcsolatos eljárási rendet, kifejezésre juttatva a rendeletben meghatározott alapelvek tiszteletét és védelmét.

Az Adatkezelő magára nézve kötelezőnek ismeri el jelen szabályzat tartalmát. Kötelezettséget vállal arra, hogy működésével kapcsolatos adatkezelése megfelel a jelen szabályzatban és a hatályos jogszabályokban meghatározott elvárásoknak.
Az Adatkezelő a személyes adatokat bizalmasan kezeli és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.
Az adatkezelő az alábbiakban ismerteti informatikai biztonsági gyakorlatát.

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az intézménynél az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak, az adatbiztonság követelményeinek az érvényesülését, az informatikai biztonság rendjét, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, rögzítse az Adatkezelő által alkalmazott informatikai biztonsági elveket, az Adatkezelő informatikai biztonsági politikáját, amelyet magára nézve kötelezőnek ismer el.
A szabályozás célja, hogy a jelen szabályzatban foglaltak alkalmazása és működtetése útján a Szombathelyi Köznevelési GAMESZ tevékenysége a gyakorlatban is megfeleljen az informatikai biztonságból eredő jogszabályi előírásoknak, biztosítsa az adatkezelésben meghatározott személyes adatok védelméhez fűződő alapvető jogok érvényesülését, az adatbiztonsági követelmények betartását, biztosítását.

A szabályozás célja továbbá, hogy meghatározza azon személyek körét, akik felhatalmazottak a Szombathelyi Köznevelési GAMESZ nevében adatkezelést végezni, illetve megakadályozza az adatokhoz történő jogosulatlan hozzáférést, az adatok törvénysértő megváltoztatását, az adatok jogosulatlanul történő felhasználását, valamint engedély nélküli nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat 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.

Az Informatikai Biztonsági Szabályzat személyi hatálya kiterjed a Szombathelyi Köznevelési GAMESZ-re, mint adatkezelőre, továbbá az adatkezelő munkavállalóira.
A Szabályzat tárgyi hatálya a Szombathelyi Köznevelési GAMESZ használatában lévő vagy általa üzemeltetett valamennyi elektronikus információs rendszerre (a továbbiakban: rendszer) és azok környezetét alkotó rendszerelemekre (adatok, szoftverek teljes körére, a folyamatokra, valamennyi telephelyére és létesítményére), az informatikai folyamatban szereplő valamennyi dokumentációra, azok teljes életciklusában kiterjed.
Jelen Informatikai Biztonsági Szabályzat 2023.01.01. napjától hatályos. Ezzel egyidejűleg valamennyi korábbi, informatikai biztonságra vonatkozó szabályzat, utasítás, egyéb eljárási rend hatályát veszíti.
Jelen Szabályzat visszavonásig érvényes, azonban a Szabályzat visszavonására kizárólag új Informatikai Biztonsági Szabályzat megalkotása esetén van lehetőség, ezzel biztosítandó, hogy az Adatkezelő tevékenysége során mindvégig érvényes és hatályos Informatikai Biztonsági Szabályzat szabályozza a tevékenységet.
A Szabályzat kidolgozásáért és az érintettek részére történt tájékoztatásért felelős a Szombathelyi Köznevelési GAMESZ igazgatója.

2. Az adatkezelés során használt fontosabb fogalmak

Személyes adat:
A meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható;

Különleges adat:
a) a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre,

b) az egészségi állapotra, a kóros szenvedélyre, a büntetett előéletre vonatkozó személyes adat;

Közérdekű adat:
Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem

eső adat;

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, illetve jogi személyiséggel nem rendelkező szervezet, 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, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelő megbízásából személyes 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.

Adatállomány:
informatikai infrastruktúrában lévő adatok logikai és fizikai összefogása, melyet egy névvel jelölnek vagy azonosítanak;

Adatátvitel:
adatok szállítása összeköttetéseken, összekötő utakon keresztül (különösen számítógépek között);
adathordozó: az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása megvalósítható;
alkalmazás: egy célfeladatot megvalósító szoftver;

Biztonságtudatosság:
A Szombathelyi Köznevelési GAMESZ biztonságáért vállalt felelősség; a meghatározott biztonsági szintnek mint követelménynek az elfogadása, illetve a hiánya következményeinek elismerése, valamint a biztonság szempontjából etikus magatartás;

Biztonsági incidens:
a rendszer működését biztonságtechnikailag hátrányosan befolyásoló, felismert és fennálló biztonsági kompromitálódás;

Dokumentum:
a rendszer által használt vagy létrehozott olyan termék, amely információt tartalmazhat, és amelyet a rendszer hozott létre vagy dolgozott fel;

Folyamatgazda:
a folyamat megtervezéséért, végrehajtásáért, ellenőrzéséért és javításáért felelős személy vagy csoport, aki figyelemmel kíséri a külső és belső szabályok betartását, az adott folyamatot értékeli, és szükség esetén javaslatot tesz a módosításokra, fejlesztésekre;

Hardver:
informatikai eszközök kézzel közvetlenül megfogható részeinek gyűjtőneve;

Hálózat:
az informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége;
hálózati aktív eszközök: a hálózat működését biztosító elektronikus elemek (különösen tűzfal, router, switch, HUB, optikai átkapcsoló);

Hálózati passzív eszközök:
a hálózati aktív eszközök kapcsolatát és kommunikációját biztosító elemek (különösen kábelezés, kábelcsatornák, fali csatlakozók és a rendezőszekrények);

Helyi rendszer:
helyi szerv által üzemeltetett és menedzselt rendszer;

Hozzáférési jog:
annak meghatározása, hogy a kezelésre jogosult milyen szoftvert, adatot vagy adathordozót kezelhet, illetve azokkal milyen műveleteket végezhet;

Információbiztonság:
olyan előírások, szabályok és szabványok betartásának eredménye, amelyek az elektronikus információs rendszerben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az elektronikus információs rendszer és elemeinek sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítását érintik, és amelyeket az informatikai rendszer alkalmazása során megelőző biztonsági intézkedésekkel lehet elérni;

Informatikai biztonság:
az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított, valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és kockázatokkal arányos, a biztonság elvárt szintje és az ezt megvalósító intézkedések jellege függ az adott informatikai rendszer biztonsági osztályától;
informatikai eszköz: minden olyan digitális eszköz és ennek funkcionális tartozéka, amely adatok összegyűjtésére, feldolgozására (rendezésére, csoportosítására, kiszámítására), előállítására, tárolására és megjelenítésére, illetve az e tevékenységekkel kapcsolatos adatmódosításra és adattovábbításra alkalmas;

Intézkedés:
a kockázatkezelés eszközei, beleértve a szabályzatokat, eljárásokat, irányelveket, gyakorlatokat, képzést vagy egyéb intézkedést, amelyek lehetnek adminisztratív, műszaki, irányítási vagy jogi természetűek;

Integritás:
a sérthetetlenségen túl a teljességet, továbbá az ellentmondás mentességet és a korrektséget jelenti, amelynek eredményeként az információ valamennyi része rendelkezésre áll, elérhető;
javítás: a hardver vagy szoftver konfigurációjának változásával, az eszközök elszállításával járó hibaelhárítási feladat;

Karbantartás:
a rendszerben vagy azok elemein végzett munka, melynek során a telepített hardver és szoftver konfiguráció nem változik, karbantartásnak minősül különösen a biztonsági réseket befoltozó hibajavítások telepítése;

Katasztrófahelyzet:
az informatikai erőforrások (különösen az elektronikus adatok, fájlok, szoftverek, számítógépek, hálózati aktív és passzív eszközök) fenyegetettsége, minden olyan nemkívánatos esemény, amely az adatok teljességét, sértetlenségét, megbízhatóságát vagy rendelkezésre állását hátrányosan befolyásolja, a fenyegetettség lehet külső esemény (tűzeset, vízkár, számítógépvírusok), vagy lehet belső tényező (hanyag kezelés, rosszindulatú adatmódosítás, szoftverhiba);

Katasztrófa:
bekövetkezett katasztrófahelyzet;

Kibertér:
a számítógépes hálózatok és az általuk összekötött számítógépek és egyéb berendezések által alkotott virtuális tér, az a környezet, amelyben az adat technikai eszközökön (számítógépes hálózatokon) keresztül áramlik, elektronikus adatok tárolódnak, online adatforgalom és kommunikáció zajlik;

Korrektív kontroll:
az eredeti állapot visszaállítását célzó intézkedés;

Operációs rendszer:
a számítógépek működésének elengedhetetlen részét képező szoftver, amelynek feladata az alapvető szolgáltatások biztosítása a programok számára, valamint az alkalmazások és a felhasználó közötti kommunikáció biztosítása;

Privilegizált felhasználó:
az a felhasználó, aki a rendszer/hálózat üzemeltetési vagy fejlesztési feladatainak végrehajtásához kiemelt jogosultsággal rendelkezik;

Privilegizált funkció:
a rendszer/hálózat üzemeltetéséhez vagy fejlesztéséhez szükséges beavatkozás;

Rendszerüzemeltető:
az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részeinek működtetését végzi, és a működésért felelős;

Szakmai adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály az adat kezelését rendeli, aki az adathoz a hozzáférési jogosultságot engedélyezi, illetve ahol az adat keletkezik;

Szerver:
szervernek minősül az olyan számítógép, amely hálózati szolgáltatásokat nyújt és/vagy kliensek kapcsolódnak hozzá;

Szoftver:
valamely informatikai eszköz olyan logikai (kézzel nem megfogható) része, amely a hardver(ek) működtetéséhez, vezérléséhez szükséges (különösen alkalmazások, operációs rendszerek);

Területi rendszer:
a területi szerv által üzemeltetett és menedzselt rendszer;

Vírus:
olyan szoftvertörzs, amely egy szoftver részeként illegálisan készült, a szoftver alkalmazása során átterjedhet, „megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói szoftvert, sokszorozva önmagát, károkat és teljes működésképtelenséget okozhat

3. Az IBSZ biztonsági besorolás

Intézményünk a 41/2015. (VII. 15.) BM rendelet, 1. mellékletében foglaltak alapján a 2. biztonsági osztályba sorolható.

4. Kapcsolódó szabályozások

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:
- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési kézikönyv.
- Közbeszerzési Szabályzat
- A közérdekű és közérdekből nyilvános adatok megismerésére irányuló igények teljesítésének rendjéről és a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló szabályzat
- Elektronikus megfigyelőrendszer üzemeltetésének szabályzata
- Iratkezelési Szabályzat
- Integrált Kockázatkezelési Szabályzat

5. Alapelvek

A felhasználó kötelessége az információvédelem területén az adott helyzetben általában elvárható magatartást tanúsítani, és tartózkodni minden károkozó tevékenységtől. Az informatikai eszköz felhasználója csak az a személy lehet, aki a Szombathelyi Köznevelési GAMESZ-szel foglalkoztatási jogviszonyban áll, a munkavégzéshez megfelelő informatikai ismeretekkel rendelkezik, valamint nyilatkozik a Szabályzatban foglaltak tudomásul vételéről. A munkaköri leírásban el kell különíteni a jogköröket és a feladatköröket az egyes személyek között annak érdekében, hogy a személyes felelősség megállapítása mindenkor biztosított legyen. Az informatikai rendszert úgy kell kialakítani, hogy biztosított legyen annak megbízható, zavartalan és folyamatos működése.
A Szombathelyi Köznevelési GAMESZ tulajdonát képező vagy használatában álló

eszközöket rendeltetésszerűen, csakis munkavégzés céljából, a tásaság érdekeinek szem előtt tartásával, a szerv által meghatározott módon, a felhasználó felelősségére lehet használni.
Az eszközök minden egyéb célú, különösen magáncélú használata a Munka Törvénykönyvének megfelelően tilos.
A felhasználó felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver- és szoftverintegritását. Az integritás sérelmének minősül a rendeltetésellenes használat, hardveres (különösen az informatikai eszközből történő alkatrész eltávolítása, illetve alkatrész behelyezése) vagy szoftveres módosítás (különösen nem engedélyezett program telepítése, a gyártói támogatással rendelkező verzió módosítása, biztonsági beállítások módosítása).

A felhasználó csak a saját azonosítójával jelentkezhet be a Szombathelyi Köznevelési GAMESZ hálózatára, másnak a saját bejelentkezési hozzáférését nem adhatja át, nem teheti lehetővé, hogy más hozzáférjen. A nem a Szombathelyi Köznevelési GAMESZ tulajdonában álló, idegen, információs, számítástechnikai és telekommunikációs eszközt az igazgató engedélye nélkül a szerv informatikai struktúrájához csatlakoztatni szigorúan tilos.

A felhasználó köteles a biztonságot támogató szoftverek használatára, azokat az általa használt eszközről nem törölheti le, nem kapcsolhatja ki, valamint kizárólag olyan szoftvereket, programokat használhat, amelyek a munkavégzés céljából szükségesek, engedélyezettek.
A felhasználó kötelessége az általa felismert biztonsági incidenst vagy az általa feltárt biztonsági sebezhetőséget haladéktalanul jelezni a rendszerüzemeltetőnek és az igazgatónak, hogy annak elhárítása a lehető leghamarabb megtörténjen.

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.

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.

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. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére biztosítani kell.

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

Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

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.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és 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.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. (1. sz. melléklet)

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 az adott lehetőségekhez mérten 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 azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

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.

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 jelszó gyakori megváltoztatásának az elmulasztása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal 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.

9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások

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

A rendszerek megvalósítása során előforduló veszélyforrások

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

A működés és fejlesztés során előforduló veszélyforrások

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

Az intézmény székhelyén és telephelyein üzemelő biztonsági kamerarendszer rögzítő egységén tárolt felvételek csak hatósági felhívásra adhatóak ki és kiadásához, felhasználásához az intézmény adatgazdájának engedélye is szükséges. Adatgazda: igazgatóhelyettes. A felvételekhez való hozzáférést biztonsági jelszó megadásával kell biztosítani.
A használó a készülék használata során köteles betartani a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényben foglaltakat, illetve figyelembe venni az adatvédelmi biztos 415/K/2009-3 ügyiratszámú állásfoglalását.

A biztonsági kamerarendszer meglétéről a vonatkozó rendeletben meghatározott tájékoztatótáblákat kell kihelyezni az intézmény bejáratánál.

10. Az informatikai eszközök környezetének védelme

Vagyonvédelmi előírások

- A számítógéppel ellátott irodák külső és belső helyiségeit zárakkal kell felszerelni,
- a számítógéppel ellátott irodákba való be- és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak a számítógéppel ellátott irodákban
- munkaidőn túl a számítógéppel ellátott irodákban csak engedéllyel lehet tartózkodni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- az irodákban a hosszabb munkaszünet idejére el kell zárni a védendő információkat tartalmazó dokumentumokat és adattároló eszközöket
- a számítógéppel ellátott irodákba történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős
- az intézmény számítógépeit jelszavas védelemmel kell ellátni
- az intézmény különböző szintű jogosultságokkal rendelkeznek, a hálózaton felhasználói név és jelszó segítségével azonosítják magukat
- az eszköz zárolásra kerül 5 perc inaktivitást követően

- selejtezés alkalmával minden adathordozó tartalmát dokumentáltan törölni kell, ezután olyan fizikai roncsolással kell megsemmisíteni, hogy újbóli használatba vétele lehetetlenné váljon
- a megsemmisítésről jegyzőkönyvet kell felvenni
- a külső adathordozóra másolás előtt a felhasználónak vírusellenőrzést kell végrehajtania a másolandó adatállományon, a forrás munkaállomáson rendszeresített vírusellenőrző programmal.

Adathordozók

- a beépített adathordozóval ellátott rendszer önmagában is adathordozónak minősül, így az adatot tároló adathordozókat védeni kell a jogosulatlan hozzáféréstől, visszaéléstől vagy megrongálódástól
- 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 más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Tűzvédelem
A Szombathelyi Köznevelési GAMESZ a rendszer védelmét a megfelelő biztonság kialakításával biztosítja. A tűzvédelmi előírásokat a Szombathelyi Köznevelési GAMESZ annak megfelelően alakítja ki, hogy az épületben milyen elektronikai rendszer üzemel.
A tűzvédelmi előírásokat az intézmény Tűzvédelmi Szabályzata tartalmazza.

Az energiaellátás biztosítása érdekében szünetmentes tápegységet is telepített.
Tilos az informatikai erőforrásokat koncentráltan tartalmazó helyiségfunkciójától eltérő anyagot vagy eszközt tárolni. AZ adatkommunikációs kábelek fizikai védelme érdekében biztosítani kell, hogy az alkalmazott technológiák védjék a kábeleket a mechanikai sérülés, elektromágneses zavarok, illegális rácsatlakozás, szándékos rongálás, szabotázs és lopás ellen.

Az informatikai erőforrásokat koncentráltan tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a gépterem és az adatállomány-tároló helyiség között.

Az intézmény azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a főbejárat mellett 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak az igazgató tudtával, ill. engedélyével szabad végezni.

A számítógéppel ellátott irodákban csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. fénymásolópapír).
Az intézmény területén dohányozni tilos!

11. A hozzáférés felügyelete

Az információhoz és az információfeldolgozó eszközökhöz való hozzáférést korlátozni kell az arra jogosultak körére. A felhasználók részére a rendszerhez történő hozzáférést a rendszer biztonsági beállításainak érvényesítése és azok ellenőrzését követően lehet biztosítani, amelyet a rendszerüzemeltető hajt végre.
A rendszernek alkalmasnak kell lenni a hozzáférési jogok egyedi vagy csoportszinten való megkülönböztetésére és szabályozására, valamint a felhasználók személyhez köthető egyedi azonosítására.

A felhasználót a rendszer egyedi azonosítóval látja el, melynek alapján nyomon követheti a rendszerben végzett tevékenységét. A rendszerhez való hozzáférést a felhasználó megbízható azonosítása előzi meg, amely a személyes használatra kiadott egyedi felhasználói névvel és ehhez tartozó, kizárólag a felhasználó által ismert jelszóval történik. A felhasználó az első bejelentkezése után köteles azonnal megváltoztatni a jelszavát. Minden felhasználónak lehetőséget kell biztosítani arra, hogy jelszavát bármikor megváltoztathassa. Amennyiben a jelszó kompromittálódásának gyanúja megalapozott, azt a felhasználó haladéktalanul köteles megváltoztatni.

Az igazgató az információbiztonság fenntartása érdekében az azonosítókat letilthatja, ha

- a jelszó kompromittálódásának gyanúja megalapozott;
- a felhasználó megsérti a rá vonatkozó adatkezelési szabályokat;
- a felhasználó foglalkoztatási jogviszonya megszűnt, szünetel vagy munkaköre megváltozott;
- A jogosultságokat a munkavégzéshez minimálisan szükséges mértékű jogosultságokra kell korlátozni, a szükséges és elégséges ismeret elvének megfelelően.

Az erőforrásokhoz való hozzáférési jogosultságok kiadásánál törekedni kell a csoportszintű jogosultságok alkalmazására. A felhasználók számára tiltani kell a következő tevékenységeket:

- BIOS hozzáférés;
- hardver telepítés;
- szoftver telepítés;
- hozzáférés a rendszerfájlokhoz (módosítás);
- rendszeridő és dátum módosítás;
- naplófájlok módosítása, törlése;
- operációs rendszer rendszerbeállításainak megváltoztatása;
- felhasználó jogainak megváltoztatása.

A rendszernek meg kell akadályoznia, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését vagy megváltoztatását. A távoli hozzáférést, a vezeték nélküli hozzáférést és a privilegizált parancsok és biztonságkritikus információk eléréséhez távoli hozzáférési jogosultság megadását az igazgató, mint adatgazda engedélyezheti. A felhasználó számára csak olyan hálózatokhoz és hálózati szolgáltatásokhoz való hozzáférés biztosítható, amelyek használata engedélyezett a számára.
A felhasználó hibájából bekövetkezett kompromitálódás vagy annak gyanúja esetén az igazgatónak vizsgálni kell a felhasználói jogosultság azonnali felfüggesztésének indokoltságát. A hozzáférési jogosultságokat az igazgató személyügyi, munkaköri változások bekövetkezésekor minden esetben haladéktalanul felülvizsgálja, és indokolt esetben

intézkedik a hozzáférési jogosultságok módosítására, visszavonására. A 90 napja nem használt felhasználói fiókot és a hozzá tartozó postafiókot az informatikai üzemeltetésért felelős vezetőnek fel kell függeszteni. A 90 napot meghaladó távollét, betegség esetén a felhasználó jogosultságait fel kell függeszteni, a helyettesítést a hozzáférési jogosultságok ideiglenes megváltoztatásával kell biztosítani.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

Az számítógéppel ellátott irodák védelme

Elemi csapás *(vagy más ok)* esetén a számítógéppel ellátott irodákban bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:
- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

Az informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses és optikai adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftver védelme. A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá 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 szervezeti egységek személyei férjenek hozzá).

A központi szerveren (//Dellserver), és a telephelyi szerveren (\\Dellserver2) létrehozott osztott mappák felhasználói jogosultsághoz kötöttek. Az adathozzáférési jogosultságok a csoportvezetők és a szakmai felettesek által kerülnek meghatározásra, akik ezt írásban engedélyezik a 4. számú melléklet alapján. Az engedélyt az informatikus hagyja jóvá informatikai szakmai szempontból és ezután ezt állítja be a szerveren.

- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

A szerver(ek) rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát zárható szekrényben kell tárolni.

Adathordozók védelme

Az üzemeltetési eljárásokat csak annak a felhasználónak lehet hozzáférhetővé tenni, akinek ez a munkaköri feladatainak ellátásához feltétlenül szükséges. Dokumentált és engedélyezett módon kell kezelni minden olyan szervezeti, folyamatbeli, az információfeldolgozó rendszerelemet és rendszerkonfigurációt, valamint a hálózatot érintő változtatást, amelyeknek hatása van az információbiztonságra.
A rendszerhez alapkonfigurációt kell összeállítani, azt dokumentálni kell, és karban kell tartani. Változatlan állapotban meg kell őrizni a rendszer alapkonfigurációját és annak előző verzióját, hogy szükség esetén lehetővé váljon az erre való visszatérés. A szükséges rendszerteljesítmény biztosítása érdekében az erőforrások használatát nyomon kell követni, optimalizálni kell és a jövőbeni kapacitásszükségletet előre kell jelezni. A felhasználónak a bekövetkezett hardverelem-meghibásodást haladéktalanul jelentenie kell a rendszerüzemeltető szervezetnek.
A Szombathelyi Köznevelési GAMESZ informatikai eszközeit a gyártó vagy a forgalmazó előírásai szerint kell karbantartani, folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében. A munkaállomások és szerverek karbantartási feladatai között ellenőrizni kell a telepített szoftverek listáját és verzióját, valamint a kritikus és biztonsági frissítések állapotát.
A Szombathelyi Köznevelési GAMESZ operációs rendszerei és a felhasználói programjai kereskedelmi forrásból beszerzett, jogtiszta programok. Az operációs rendszer és alkalmazás verzióját, valamint biztonsági patch szintjét tesztelést követően lehetőség szerint a gyártói támogatással rendelkező, legmagasabb szintre kell hozni.
A rendszert úgy kell beállítani, hogy a működése során keletkező nem nyilvános maradvány információk (különösen az átmeneti fájlok) bizalmasságát, sértetlenségét védje. Az informatikai üzemeltetésért felelős vezetőnek a rendszer minden arra alkalmas – megfelelő hardver- és szoftverkörnyezettel rendelkező – elemére jóváhagyott vírusellenőrző szoftvert kell telepítenie és naprakészen tartania.

Az adathordozón látható módon fel kell tüntetni, hogy vírust, kártékony kódot tartalmaz. A kéretlen és kártékony kódot tartalmazó elektronikus levelek kiszűrésére olyan központilag menedzselt szűrőt kell üzemeltetni, amely automatikusan központilag frissíti az adatbázisát, és frissíti a rendszert új verziók elérhetővé válásakor.

A biztonsági mentés célja az információ és az adatfeldolgozó szoftverek épségének és rendelkezésre állásának biztosítása. A hatékony biztonsági adatmentés érdekében a munkaállomásokon feldolgozott adatállományokat tárolni kizárólag szervereken és központi kiszolgálókon, valamint az adatmentésre szolgáló médián lehet. Bármilyen más helyen történő adattárolás még átmenetileg is tilos. Az adatvesztés elkerülése érdekében a Szombathelyi Köznevelési GAMESZ az alábbi módon végez biztonsági mentést: a szerveren elhelyezkedő osztott könyvtárban tárolt közösen használt dokumentumok mentését kétnapi gyakorisággal (kedd, csütörtök) a rendszergazda végzi el a Nádasdy szerverről egy külső merevlemezes adathordozóra, a Boglárka úti szerverről NAS egységre. A mentés során generációs mentési mechanizmust alkalmaz, amelynek értelmében az adatok a következőképpen archiválandó:

- 1 hétre visszamenőleg a hét első mentése,
- 1 hónapra visszamenőleg a hónap első mentése,
- 1 évre visszamenőleg pedig az év első mentése kerül archiválásra.

A rendszergazda a mentés megtörténtét egy kézzel írt naplóban vezeti, melyben rögzítésre kerül a mentés dátuma, típusa, melynek megtörténtét a rendszergazda aláírásával igazolja. Az idő elteltével esetlegesen – az adathordozó kapacitása miatt - törlésre kerülő mentéseket

a naplóból áthúzással törölni kell.

A biztonsági mentések gyakorisága és tartalma alkalmas arra, hogy megelőzze a személyes adatokkal kapcsolatos adatvesztést.

A Szombathelyi Köznevelési GAMESZ minden olyan adatot ment, amely az auditálás, ellenőrzés eszköze lehet (különösen naplófájlok, riportok). Ezeket az adatokat a többi felhasználói, illetve rendszer adattól elkülönítetten menti, és minimum öt évig megőrzi.

A naplóbejegyzések vizsgálatát, elemzését és jelentését integrált folyamattá kell alakítani, amely a veszélyes vagy tiltott tevékenységekre és történésekre megfelelően képes reagálni. A rendszernek naplóznia kell a felhasználói tevékenységet, valamint a privilegizált felhasználó privilegizált jogosultsággal végzett tevékenységeit. A naplózó eszközt, illetve a naplóinformációt meg kell védeni a jogosulatlan hozzáféréstől, törléstől, kiiktatástól vagy módosítástól.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

Adathordozók tárolása
Az adathordozók tárolására a géptermen kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

Adathordozót a részlegből ki-, illetve oda bevinni csak a *csoportvezető* engedélye alapján lehet. Az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet.

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.

Selejtezés, sokszorosítás, másolás
Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, külső adathordozót, CD-t, pendrive-ot, külső HDD-t.
- véglegesen elhasználódott anyagot.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni.

13. A hálózat biztonsága

A hálózatüzemeltetőnek a rendszer hálózati elemeit menedzselni és felügyelni kell. A hálózatmenedzsment segítségével kell megoldani a hálózatok biztonságát és az infrastruktúra védelmét. Olyan ellenőrző-felügyeleti eszközöket kell használni, amelyek biztosítják a hálózatokban kezelt és továbbított adatok biztonságát, és megóvják a hálózatot a jogosulatlan hozzáférésektől.
A Szombathelyi Köznevelési GAMESZ hálózatából más hálózatba csak előre definiált és a hálózatüzemeltető által engedélyezett módon szabad csatlakozni. A Szombathelyi Köznevelési GAMESZ gondoskodik a hálózati eszközökön a naplózás beállításáról és a hálózati eszközök rendszer idejének szinkronizálásáról.
Tilos a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése. A hálózat nem használható az alábbi tevékenységekre:

- a jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így mások személyiségi jogainak megsértése (különösen rágalmazás), tiltott haszonszerzésre irányuló tevékenység (különösen piramisjáték), szerzői jogok megsértése (különösen szoftver nem jogszerű terjesztése);
- profitszerzést célzó (különösen kriptovaluta bányászat), direkt üzleti célú tevékenység és reklám;
- a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybe vevő tevékenység (különösen nem hivatali körlevelek, hálózati játékok, kéretlen reklámok);
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, eszközök és szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása (különösen TCP port scan);
- a hálózat erőforrásainak a hálózaton elérhető adatoknak illetéktelen kezelése, módosítása, elérhetetlenné tétele, törlése vagy bármely károkozásra irányuló tevékenység;
- másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (különösen pornográf anyagok közzététele);
- hálózati üzenetek, hálózati eszközök hamisítása, olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

A hálózat külső határán aktív hálózati forgalom vizsgálatára és hálózati támadás felismerésére alkalmas tűzfalat kell üzemeltetni. A Szombathelyi Köznevelési GAMESZ-nél a számítástechnikai hálózatot a városi hálózati rendszer tűzfala védi. Az aktív hálózati elemeket (routerek) SZMJV Polgármesteri Hivatal által megbízott szolgáltató üzemelteti.
A tűzfal alkalmas arra, hogy az esetleges külső támadásoktól, behatolásoktól megvédjék a számítástechnikai rendszert.
Minden külső infokommunikációs szolgáltatás használatakor felügyelt interfészt kell működtetni, amelyekhez forgalomáramlási szabályokat kell meghatározni és működtetni. A szabályok meghatározásánál az alapeseti visszautasításból kell kiindulni.
Az elektronikus levelező rendszert SZMJV Polgármesteri Hivatal által megbízott szolgáltató üzemelteti.
Az elektronikus levelező rendszer elemeiről, különösen a szerverek fizikai, logikai védelméről folyamatosan gondoskodni kell. Az elektronikus levelező rendszeren keresztül történő támadások esetén, amennyiben a rendszer védelme átmenetileg nem biztosított – különösen olyan vírustámadás esetén, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet – az elektronikus levélforgalmat az informatikai üzemeltetésért felelős vezetőnek ideiglenesen le kell állítani.

14. Biztonsági események kezelése

Biztonsági eseménynek kell tekinteni minden olyan nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági kockázatot, amely veszélyeztetheti a Szombathelyi Köznevelési GAMESZ tevékenységét, és fenyegetheti az információbiztonságot, továbbá minden olyan tevékenységet vagy mulasztást, amely az utasítás be nem tartásával biztonsági eseményt eredményezhet. A biztonsági eseménykezelési folyamatra olyan rendszert kell alkalmazni, amely támogatja az alábbi tevékenységeket:

- a biztonsági esemény jelentése;
- a biztonsági eseménnyel kapcsolatos információk gyűjtése;
- tudásbázis kiépítése;
- azonnali válaszlépés meghatározása;
- azonnali válaszlépés végrehajtása;
- átfogó válaszlépés szükségességének a meghatározása;
- javaslat kidolgozása az átfogó válaszlépésre;
- átfogó válaszlépés engedélyezése;
- átfogó válaszlépés végrehajtása;
- a végrehajtás leellenőrzése;
- a biztonsági esemény dokumentálása;
- biztonsági esemény kezelési képességek dokumentált tesztelése;
- statisztikai kimutatások készítése.
- Biztonsági esemény felfedezése vagy gyanúja esetén a felhasználónak az eszközt haladéktalanul le kell választani a hálózatról, és értesíteni kell az igazgatót. Ha a biztonsági esemény fokozott kockázatra utal, akkor az igazgató intézkedik annak kivizsgálására.

15. Használatban levő programok, szoftverek a Szombathelyi Köznevelési GAMESZ-nél

a.) 001

Központosított Illetmény-számfejtési Rendszert **KIRA** intézményi modulja. A munkaállomásokon való működés alapfeltétele az intézmény-specifikus kulcsállomány megléte. A kulcsállomány archiválásra került optikai adathordozóra, így fájlsérülés esetén reprodukálható, csakúgy, mint a telepítő állományok. Az adatbázis mentése a központi számfejtési szerv a Magyar Államkincstár feladata, mivel fizikailag ez a központi szerveren helyezkedik el. A KIRA működésének másik alapfeltétele a mindenkori internet kapcsolat biztosítása.

A KIRA vonatkozásában a bér- és humánerőforrás csoport vezetője superuser (intézményi rendszergazdai) szerepkörrel rendelkezik a csoport által kezelt intézmények felett. A KIRA program esetében a bér- és humánerőforrás csoport vezetőjének a hatáskörébe és felelősségi körébe tartozik a felhasználói jogosultságok meghatározása, kiosztása, valamint a kulcsfájlok számítógépre való telepítésének meghatározása, továbbá szükség esetén a felhasználói jelszavak nullázása, (reset-elése).

A Központosított Illetmény Számfejtési Rendszerben 2019. május 06-tól bevezetésre került a kétfaktoros (2F) azonosítási folyamat. A KIRA, 2 faktoros belépéséhez e-személyi - kártyaolvasó használata szükséges.

A KIRA rendszer és az e-személyi-kártyaolvasó, irodán kívüli használata igazgatói engedélyhez kötött és visszavonásig érvényes. A személyügyi adatokat a felhasználók a mindenkor érvényes törvényi szabályozások figyelembevételével kezelhetik a tőlük elvárható legnagyobb gondossággal.

b.) 002

2020. január 1-től intézményünk áttért a HESSYN programról a **AndiT** Tárgyieszköz nyilvántartó programra. A Hessyn záróállományainak adatmigrációja megtörtént az **AndiT** Tárgyieszköz nyilvántartó program nyitóállományába. A migrációt követő adatellenőrzést a programot kezelő munkatársak elvégezték.

Cégnév:	Andit Solutions Kft.
Név:	Guethné Horváth Andrea
Telefon:	+36 70 671 4858
E-mail cím:	info@andit.hu
Rendeltetés:	Tárgyi eszköz nyilvántartás
Tárolt adatok köre:	Kis- és nagyértékű tárgyi eszközök
Használt adatbáziskezelő:	Borland Database Engine (BDE)
Program telepítve:	Boglárka u.2. szerver (192.168.0.1)
Jogosultak nevei:	- Szilvágyi Andrea - Némethné Szigetvári Dóra

2020. január 1-től bevezetésre került az AndiT tárgyieszköz nyilvántartó program, amelyet a GAMESZ kis- és nagyértékű tárgyi eszközeinek nyilvántartására használunk.
A program a GAMESZ 9700 Szombathely, Boglárka u.2. telephely alatt található szerveren, a \\192.168.0.1\WINSERVER2\Data\Share\AndiT\TARGYI nevű, megosztott mappában található, ebbe a mappába kerülnek a program biztonsági adatbázis mentései is. A mappáról hetente kétszer (kedd és csütörtök) a rendszergazdák által készül külső adathordozóra biztonsági mentés.
A program támogatását az Andit Solutions Kft biztosítja, akinek saját használatra átalakított, távelérésre alkalmas szoftverének (TeamViewer) hordozható verziója a kliensszámítógépen található. Igény esetén a rendszergazdák értesítése és igény szerinti jelenléte mellett az ügyintéző a fejlesztővel telefonon felveszi a kapcsolatot, aki a távelérés aktiválásával biztosítja a kért szoftvertámogatást.

c.)003

A DOKK programot 2014.01.01-én felváltotta a Korend Rendszerház Kft (2800 Tatabánya, Mártírok útja 12. 3/3, Telefon/fax: +3634 309-021, mobil: +3620 220 3419, Adószám: 13666387-2-11, Cégjegyzék száma: 11-09-011392) vállalkozó által fejlesztett, **GORDIUS Pénzügyi Információs Rendsze**r. A Korend Kft. által biztosított GORDIUS könyvelési rendszer az önkormányzat fájlszerverén helyezkedik el. Elérése távoli asztali kapcsolattal történik. A rendszer integrált funciókkal rendelkezik, számlázó programként használható. A felhasználói dokumentáció és az aktuális változások a Korend Kft által megküldésre kerül, melyet a GAMESZ, központi szerver osztott mappájában („\\192.168.0.1\Kozos\Dokumentációk /Gordius dokumentáció mappában) minden dolgozó részére hozzáférhetővé teszünk.
Az GORDIUS Pénzügyi Információs Rendszer adatbázis mentését a Polgármesteri Hivatal Informatikai Irodájának - a központi adatbázisszerverhez rendszergazdai joggal rendelkező - megbízott dolgozója végzi. A GORDIUS programnak és moduljainak felhasználói, hozzáférési jogosultságainak meghatározása és kezelése a gazdasági igazgatóhelyettes hatásköre és felelőssége.

d.) 004
Költségvetés Gazdálkodási Rendszer K11 KTR almodulja.

Az adatbázis mentése a központi számfejtési szerv a Magyar Államkincstár feladata, mivel fizikailag ez a központi szerveren helyezkedik el. A **KGR K11** működésének másik alapfeltétele a mindenkori internet kapcsolat biztosítása.

e.) 005
Az Unicredit Bank által biztosított **Spectra** ügyfélprogram mentési mappája az intézményi fájlszerveren helyezkedik el. A mappáról hetente kétszer (kedd és csütörtök) a rendszergazdák által készül külső adathordozóra biztonsági mentés. A Spectra felhasználói hozzáférés szabályozásáért a gazdasági igazgatóhelyettes felelős-, működtetéséért a pénzügyi és könyvelési csoportvezető a felelős személy.

f.) 006
Raktár Start program

Név: Naturasoft Raktár Start
Cégnév: Naturasoft Magyarország Kft.
Bevezetés: 2016.01.01.
Hely: Nádasdy Ferenc u. 4. (WINSERVER3) szerveren található
Adatbázis: SQL
Mentés: Kedd- Csütörtök
Felhasználók: Bata Adrienn
Sifter József
Lovász Zoltán
Szandi Zoltán

2016.01.01-től bevezetésre került a Naturasoft Magyarország Kft. (1113 Budapest, Bocskai út. 77-79., telefon: +36 1 209-2152) vállalkozó által fejlesztett, Naturasoft Raktár Start raktárkezelő program. A Naturasoft Magyarország Kft. által biztosított Raktár Start raktárkezelő szoftver adatbázisa a Nádasdy Ferenc u. 4. (Dellserver2) szerveren található, melyről a rendszergazda a heti mentések alkalmával (kedd-csütörtök) szintén biztonsági mentést készít. A kompetens személyek számítógépén a Raktár Start kliens verziója került telepítésre, melynek köszönhetően a szerverhez(Dellserver2) csatlakozva egy adatbázisban akár többen is tudnak tevékenykedni. A felhasználók egyedi felhasználó névvel, illetve ehhez tartozó jelszóval rendelkeznek. A felhasználói, hozzáférési jogosultságok meghatározása az anyaggazdálkodási csoportvezető és az igazgatóhelyettes hatáskörébe tartozik.

g.) 007

2015.09.01-től bevezetésre került a Yami Bt. – Gáspár Csaba EV Adószám: 67460614-1-34 - programfejlesztő (8638 Balatonlelle, Szélső u. 9., mobil: +36 30 990-8336) mint szolgáltató - vállalkozó által fejlesztett, **Menzasoft III étkezés-nyilvántartó, számlázó program**.

A MenzaSzoft III. étkezésnyilvántartó program 2018. február 01-től kezdődően folyamatosan bevezetésre került 18+1 szombathelyi óvodában, így összesen 19 óvodai és 10 db iskolai- és kollégiumi- programot futtató számítógép működik. 2021. június 15-től ezeken a számítógépeken a MenzaSzoft III program kliens verziója működik, kivéve az Aranyhíd EGYMI Micimackó Óvodában működő számítógép, melyen továbbra is a helyi háttértárolón helyezkedik el az adatbázis, illetve a MenzaSzoft III. program.

2021. június 15-től az étkezésnyilvántartó program intézményi adatbázisai, valamint a szerver oldali program és adatbázisszerver, SZMJV Polgármesteri Hivatal Informatikai Irodája által üzemeltetett szerver számítógép háttértárolóján kerültek elhelyezésre.
A szolgáltató által biztosított Menzasoft III étkezési kliensszoftver az intézményt kezelő étkezési ügyintéző hordozható számítógépére, óvodai programhasználat esetén az óvodatitkár számítógépére kerül telepítésre.

2023. január 01-től MS SQL iskolai-kollégiumi adatbázisra épülő programverzió került bevezetésre **MENZA MS** néven.

A napi gyakoriságú, teljes adatbázismentésről, a mentések archiválásáról, az adatvédelmi rendeleteknek megfelelő őrzéséről és visszaállíthatóságáról SZMJV Polgármesteri Hivatal Informatikai Irodája gondoskodik.

A rendszer számlázó programként használható. A számlázó program bejelentési kötelezettségének teljesítése a Nemzeti Adó és Vámhivatal rendszerébe a Szombathelyi Köznevelési GAMESZ gazdasági igazgatóhelyettesének feladata.

A felhasználói dokumentációt és az aktuális változások dokumentációját a szolgáltató biztosítja, melyet a GAMESZ, Szombathely, Boglárka u.2. telephelyén a központi szerver osztott mappájában, a következő elérési helyen:
„\\192.168.0.1\Kozos\Dokumentációk\MenzaSzoft_dokumentáció" minden dolgozó részére hozzáférhetővé teszünk.

A számítógép kezelőnek biztosítania kell a használatában levő számítógép vagy hordozható számítógép fizikai védelmét. A számítógépet csak kulccsal elzárt helyiségben vagy amennyiben lehetőség van rá, a hordozható számítógépet páncélszekrényben hagyhatja magára.
Óvodák esetében egyedileg szabályozni kell a számítógéphez való hozzáférés lehetőségét és a programot kezelő személyek körét, az adatvédelem figyelembevételével.

A logikai védelem két illetve három faktoros:

1. Meghajtótitkosítás a hordozható számítógépek-notebookok esetében *(lásd: h.008. pont)*
2. A számítógép operációs rendszerének védelme felhasználónévhez kötött, jelszóval biztosított.
3. Ugyanígy a programba való belépés is felhasználónévhez kötött, jelszóval biztosított. A jelszavaknak megfelelő bonyolultságúnak kell lenni: legalább 8 karakter hosszú, tartalmaznia kell kisbetűt, nagybetűt és számot is.
4. A MenzaSzoft III és a MENZA MS program superuserei, az étkeztetési csoportvezető és helyettes a saját felhasználói jogosultságaikat, és az intézményi felhasználók jogosultságait kezelik, létrehozzák, módosítják, illetve törlik.
5. Az iskolai intézményi adatbázisok (általános iskolai, középiskolai, gimnáziumi, kollégiumi intézmények) tekintetében a felhasználói jogosultságokat a központi felhasználó (superuser), - jelen esetben az étkeztetési csoportvezető engedélyezi és a rendszergazda segítségével ő állítja be.
6. Az óvodai intézményi adatbázisok felhasználóit az óvodavezetők határozzák meg. A hozzáférési jogosultságokat a 9. melléklet felhasználó menüpontban megadottak szerint az étkeztetési csoportvezető engedélyezi és a rendszergazda állítja be.

A rendszerszintű és programszintű jelszavakat csak a kezelő tudhatja. A jelszavakat minden esetben lezárt borítékban a kezelő intézményének telephelyén páncélszekrényben kell őrizni, biztosítva a boríték sértetlenségét aláírással és felülbélyegzéssel. A boríték felbontását csak az igazgató rendelheti el. A felbontásról jegyzőkönyvet kell készíteni.

Használaton kívül a MenzaSzoft III. programot szabályosan be kell zárni, a számítógépet, hordozható számítógépet pedig operációs rendszer szintjén zárolni kell olyan módon, hogy a feloldás kizárólag az egyedi felhasználónév és jelszó használatával legyen lehetséges.
Kizárólag a rendszergazdának van adminisztrátori jogosultsága a számítógépek rendszerszoftveréhez (operációs rendszerhez). A rendszerszoftverek (operációs rendszerek) felhasználói jogosultságait csak a rendszergazda változtathatja meg.

A Szombathelyi Köznevelési GAMESZ étkeztetési feladatkörébe tartozó 24 db iskolai és kollégiumi kliensprogramot és archív adatbázist működtető 10 db hordozható számítógép hardver, szoftver- és adat-védelme a Szombathelyi Köznevelési GAMESZ, - adott számítógépet használó - étkezési ügyintézőjének a feladata, a hardver-, szoftver-, és adat-védelem betartatása és ellenőrzése az étkeztetési csoportvezető feladata.

Az óvodai programot működtető 19 db számítógép hardver, szoftver- és adat-védelme az adott óvoda óvodatitkárának a feladata, a hardver-, szoftver-, és adat- védelem betartatása és ellenőrzése az adott óvoda vezetőjének a feladata.
A GAMESZ részéről az óvodai adatbázisokhoz való korlátozott hozzáférési jogosultsága mindenkor az óvodatitkárok munkáját koordináló GAMESZ ügyintézőnek, illetve annak – a munkaköri leírásában szereplő GAMESZ ügyintézőnek van, aki az óvodai étkezési nyilvántartásban szereplő gyermekek részére megrendelt havi adagokat összeveti a mulasztási naplóban rögzített tényleges jelenlétekkel.
A hozzáférési jogosultságokat az étkeztetési csoportvezető engedélyezi, a rendszergazda állítja be.
GAMESZ ügyintéző tartós távolléte esetén az étkeztetési csoportvezető, a „Helyettes" felhasználóval engedélyezi az óvodai adatbázishoz való korlátozott hozzáférést a helyettesítő GAMESZ munkatárs részére.

Az óvodatitkár, óvodai felhasználók, valamint a GAMESZ ügyintézők, központi felhasználók programon belüli jogosultágait (funkciókhoz, adatokhoz való) hozzáférését a 9 - 10. mellékletek tartalmazzák.

h.) 008
Meghajtótitkosítás
Az étkeztetési csoport hordozható számítógépjein, valamint az óvodák óvodatitkári számítógépein üzemel az étkezésnyilvántartó-számlázó MenzaSzoft III. elnevezésű program, mely adatbázisa a központi önkormányzati szerveren, illetve a lokális háttértárakon van tárolva.
A számítógépek közül a hordozható számítógépeknek háttértára a Windows által biztosított Bitlocker alkalmazás használatával kerül titkosításra. A titkosítás a lokális meghajtó teljes adatterületét érinti, az adatok módosítása esetén az újonnan felvitt adatok automatikusan titkosításra kerülnek.
A titkosítás 256 bit-es XTS (Xex cipherText Stealing) módú AES (Advanced Encription Standard - 1619-2007 IEEE szabvány a blokkorientált tárolóeszközök adatainak kriptográfiai védelméről) szabványú algoritmussal valósul meg.
Jelszó:
A titkosítás feloldásához a számítógép a bekapcsoláskor további hitelesítést követel meg, amelynek jelen esetben egy, a számítógép kezelője által megadott és a rendszergazda által beállított jelszó beírásával tehetünk eleget. A jelszó házirendje a következő:

- minimum 8 karakter hosszúságúnak kell lennie,
- tartalmaznia kell nagy-, kis betűt és számot,
- nem egyezhet meg a Windowsba való belépéshez használt jelszóval,
- a jelszó megadásánál figyelembe kell venni, hogy a feloldáskor a rendszer csak angol billentyűzet szerinti beírási módot támogat.

A Bitlocker jelszava módosítható, a módosítást az adott szervezeti egység csoportvezetője kezdeményezheti, jegyzőkönyv készül róla, és a későbbi visszafejtést lehetővé téve rögzítésre kerül.

Feloldókulcs
Jelszó hiányában a titkosítás a merevlemezen csak egy, a titkosítás előtt kinyomtatott feloldókulccsal lehetséges.

- a feloldókulcs kinyomtatásra, majd a fentiek szerint beállított jelszó mellé, lezárt borítékban a páncélszekrénybe kerül,
- a borítékra rögzíteni kell a felhasználó nevét, a gép típusát és gyári számát.
- a boríték későbbi felhasználásra páncélszekrényben tárolandó, amely csak az igazgató engedélyével nyitható fel.

Meghajtótitkosítással (bitLocker) biztosított hordozható számítógépek:

Név		Számítógép	
		Típus	Gyári szám
1.	Prikazovics Judit	Dell Vostro 15	8R4STJ2
2.	Tóth Tiborné	Dell Vostro 3580	1PPX5Z2
3.	Hajnal Kornélia	Dell Vostro 15	9S4STJ2
4.	Nagy Marietta	Dell Vostro 3580	2RTD723
5.	Gőcze Gáborné	Dell Vostro 3580	9TTD723
6.	Éder Tiborné	Dell Vostro 15	JR4STJ2
7.	Szilvágyiné Szalay Erika	Dell Vostro 15 3000	7S4STJ2
8.	Kárer Barbara	Dell Vostro 3580	3RPX5Z2
9.	Sziklai Amanda	Dell Inspiron 15 3000	5KKC832
10.	Csigó Tímea (Micimackó Óvoda)	Dell Inspiron 15	4SNXCW1
11.	Serleginé Borbás Anikó (Kőrösi)	HP 250 G6	CND8134CLC
12.	Gyöngyössyné Andrea (Pipitér)	HP 250 G6	CND8134CLL
13.	Tömőné Nardai Anita (Benczúr)	HP 250 G6	CND8134CLB

i) 009
IRMA iktatórendszer

Köznevelési GAMESZ az iratkezelést osztott iratkezelési szervezetben (kettő telephely) látja el. A Köznevelési GAMESZ a sávos iktatást alkalmazza, minden szervezeti egység (csoport) rendelkezik egy sávos számkerettel. A szervezeti egységek számkeretén belül az iktatási számok formátuma: főszám + alszám / év. Az iktatás elektronikus úton történik az AC Soft Kft. (Székesfehérvár, Géza u. 32.) által készített IRMA ügyiratkezelő rendszerrel.

Az iratkezeléssel kapcsolatos feladatok (a továbbiakban: iratkezelés) irányítását a humánerőforrás és bérügyi csoportvezető látja el. A központi irattárral, iratselejtezéssel

és levéltári iratátadással összefüggő feladatok irányítását, felügyeletét a gazdasági igazgatóhelyettes látja el.

Az iktatórendszerhez való hozzáférési jogosultságokat névre szólóan kell dokumentálni, amelyet az informatikai és biztonsági szabályzat 8. számú melléklete tartalmaz.
A jogosultságok regisztrálását, beállítását, illetve módosítását, megvonását a szervezeti egység vezetőjének kell írásban kezdeményezni a SZMJV Polgármesteri Hivatal Informatikai, Irodájánál (továbbiakban Informatikai Iroda).

Az Informatikai Iroda köteles gondoskodni az iratkezelési szoftver által kezelt adatok biztonságáról, s megtenni azokat a technikai és szervezési intézkedéseket, kialakítani azokat az eljárási szabályokat, amelyek az üzembiztonsági, adatvédelmi szabályok érvényre juttatásához szükségesek. Az iratokat és az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, valamint a megsemmisülés és sérülés ellen.

2022. január 01-ől bevezetésre került az IRMA rendszeren belül az e-számlaérkeztetési funkció. Az e-számlák érkeztetését 2023.01.01-től a Szombathely, Nádasdy u. 4. és Boglárka u 2. irodában két helyen végzik a 7. mellékletben meghatározott jogosultságok alapján.

j) 010
ESET NOD32 vírusvédelmi és biztonsági szoftver:
A szerverek és a munkaállomások, notebookok védelmének biztosításához

Szolgáltató:
Sicontact Kft.
H-1106 Budapest, Örs vezér tere 25/C
Árkád Irodaház 4. emelet
Tel.: +36-1-346-7052
Fax: +36-1-999-7977
E-mail: info@sicontact.hu

GAMESZ munkaállomások
ESET Endpoint Antivirus Workstation Protection
100 számítógépre szóló évente megújított licence

GAMESZ szerverek
ESET File Security for Microsoft Windows Server
2 szerverre szóló évente megújított licence.

Felelős rendszergazdák:

Szombathely, Nádasdy u. 4. székelyen a szerver (Dellserver), a munkaállomások, valamint az étkezési csoport hordozható számítógépeinek tekintetében: Szandi Zoltán, helyettese a kijelölt rendszergazda.

Szombathely, Boglárka u. 2. telephelyen a szerver (Dellserver2) és munkaállomások tekintetében: Szandi Zoltán, helyettese a kijelölt rendszergazda.

Szoftver védelem
Rendszerszoftver védelem
A rendszerszoftvereket naprakész állapotban kell tartani, ami az automatikus frissítési szolgáltatás beállításával érhető el.

Teendők a következők:

- az üzembiztonság érdekében operációs rendszer biztonsági másolatával kell rendelkezni, amely szükség esetén azonnal betölthető legyen,

- Ki kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek:

Kijelölt személyek a rendszergazdák.

- a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni.

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, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.
Lokális gépekre programot csak a rendszergazda tudtával lehet telepíteni.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.
A programokról nyilvántartást kell vezetni, amelynek. legalább az alábbi adatokat kell tartalmaznia:
- a program azonosítója,
- a program készítőjének neve,
- a program megnevezése.
(5. számú melléklet)

16. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy azok megismétlődjenek.

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

Az Informatikai Biztonsági Szabályzat

2023. január 01. napjával lép hatályba.

1. sz. melléklet

Szombathelyi Köznevelési GAMESZ
Székhely: Szombathely, Nádasdy F. u. 4.
Telephely: Szombathely, Boglárka u. 2.

ADATKEZELÉSI NYILATKOZAT

Alulírott.....
(név ,lakcím)
nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a munkavégzéshez szükséges adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek.

A számítógépek háttértárolóján csak a munkavégzéshez szükséges adatok, fájlok programok tárolhatók, különös tekintettel tilos bármilyen illegális tartalom, médiatartalom letöltése, tárolása és felhasználása.
Az adatbiztonság, és jogszerű adattárolás megtartásáért a mindenkori számítógép kezelője, a felelős személy.

A fentieket megértettem, büntetőjogi felelősségem tudatában magamra nézve kötelezőnek tartom.

Dátum: 20.....

.....
aláírás

2. *sz. melléklet*

Számítógéppel ellátott irodák rendje

1. A Számítógéppel ellátott irodákban az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:

- az intézmény igazgatója, helyettesei
- csoportvezetők
- az igazgató által kijelölt személyek
- rendszergazdák

Más személyek benntartózkodását csak az igazgató engedélyezheti.

2. Üzemeltetés alatt az ajtókat állandóan becsukva, üzemidőn kívül pedig zárva kell tartani. Munkaidőn, kívül idegen személy csak az intézmény igazgatójának (távollétében helyettesének) engedélyével tartózkodhat számítógéppel ellátott irodákban.
A számítógéppel ellátott irodák áramtalanításáért a számítógép kezelő a felelős.

3. Az számítógéppel ellátott irodákban az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni.

4. A számítógépek közvetlen közelében ételt, italt fogyasztani TILOS!

5. SZIGORÚAN TILOS számítógéppel ellátott irodákba égő cigarettával belépni, illetve ott dohányozni!

6. A számítógéppel ellátott irodák takarítását csak az arra előzőleg kioktatott személyek végezhetik.

7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazda végezhet.
Ez alól csak a szervizek szakemberei kivételek.

8. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.

9. Az számítógéppel ellátott irodákban elhelyezett adathordozókhoz *a gépkezelőkön* kívül, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.

10. Adathordozókat és iratokat csak a gépkezelő engedélyével lehet kihozni, illetve bevinni a gépterembe.

11. Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet!

12. A javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a munka-baleset- és tűzvédelmi előírásokat.

3. sz. melléklet

Informatikai biztonsági útmutató

Az intézmény informatikai szoftver-hardver védelmének eszközeit az Informatikai Biztonsági Szabályzat (IBSZ) foglalja magában. Ez minden dolgozó számára kötelező érvényű. Az IBSZ hozzáférhető a gazdasági igazgatóhelyettesi irodában, illetve elektronikus formában a kiszolgáló számítógép osztott könyvtárában. Az „Informatikai biztonsági útmutató" az IBSZ mellékletét képezi.

Az informatikai rendszer biztonsága érdekében a következő veszélyforrásokra kell különösen ügyelni:

1. **Külső adathordozókról történő adatátvitel** a számítógép háttértárolójára. (CD-ről, pendrive-ról, stb.)
Minden esetben az állomány megnyitás, másolás előtt kötelező a víruskeresés.

2. **Internet weboldalak megnyitása:** Csak a biztonságos adattartalommal rendelkező, illetve a munkavégzéshez kapcsolódó, vagy belső hálózaton tárolt intézményi weboldalakat szabad megnyitni. Szigorúan tilos az illegális fájlcserélő, tiltott tartalommal rendelkező weblapok megnyitása, különös tekintettel a médiatartalmakra (mp3, filmek, képek)
- audio: MP3, WAV, stb.
- video: AVI, MPG, MP4, WMV, MKV, stb.
- kép: JPG, PNG, BMP, stb.

3. A nem beazonosítható úgynevezett **hivatkozás (link)** megnyitása nagy veszélyt rejt magában, mivel olyan káros tartalmú internetes oldalra irányíthat, ami vírust, kártevőt tartalmaz. Ezek a hivatkozások lehetnek weblapokon, megkaphatók e-mailben, chat site-okon vagy akár skype-on, messenger-en és más üzenetküldőn.

4. Csak olyan **e-mailt** nyissunk meg, amely feladóját ismerjük, viszont ebben az esetben is óvatosan kell eljárni, mert egyes esetekben adathalász weboldalak, „cégek" saját ismerősünk által küldött üzenetként megjelenő e-mailjei is előfordulnak a postafiókunkban. Az ilyen e-mailek a gyanútlan felhasználót a bennük található linkre, vagy gombra kattintásra utasítják, amit követően azonnal indul a vírus, kémprogram telepítése a számítógépre.
Amennyiben gyanús levelet kapunk azonnal töröljük és a törölt elemek közül is távolítsuk el. E-mail-ben kapott csatolt állományt semmiképpen ne nyissuk meg közvetlenül. Először a Fájl mentése lehetőséggel mentsük a számítógép háttértárolójára egy külön mappába, majd a megnyitása előtt víruskeresést kell rajta végrehajtani.

Összefoglalva a veszélyforrások:
- nem biztonságos weblap
- külső adathordozók
- veszélyes hivatkozások !!!
- e-mail-ek, különös tekintettel a csatolt állományokra

A számítógépek háttértárolóján csak a munkavégzéshez szükséges adatok, fájlok programok tárolhatók, különös tekintettel tilos bármilyen illegális tartalom, médiatartalom letöltése, tárolása és felhasználása.
Az adatbiztonság, és jogszerű adattárolás megtartásáért a mindenkori számítógép kezelője, a felelős személy.

4. sz. melléklet

KÖZÖS HASZNÁLATÚ ADATOK ELÉRÉSI ENGEDÉLYE

Dolgozó neve:

Dolgozó beosztása:

Mappa \\Dellserver\ 192.168.0.1	Engedélyek – Boglárka u. 2. szerver		
	Teljes	Olvasás	Visszavon
AndiT			
Iktatás_scan			
ellenőrzés			
gazdighkönyvelés			
igazgató			
munkaügy			
Könyvelés			
Belső ellenőrzés			
Gazdigh			
Közös			
Munkaügy			
GAMESZ			
Spectra			

Mappa \\Dellserver2\ 192.168.1.12	Engedélyek – Nádasdy szerver		
	Teljes	Olvasás	Visszavon
Étkezés			
Étkezés scan			
Műszaki			
Beruházás			
Energetika			
Gépjármű ügyintézés			
Informatika			
Műszaki közös			
Vagyongazdálkodás			
Adminisztráció			
Anyagkönyvelés			
Beszerzés			
Tárgyi eszköz			
Vagyongazdálkodás közös			
Továbbszámlázás			
Scan			

Menzaszoft engedély Óvodai:.....

Menzaszoft engedély Iskolai:.....

IRMA engedély:.....

GORDIUS engedély:.....

Kelt: Szombathely, 20.... ....

....

Felelős engedélyező (felettes)

Informatikai jóváhagyó

5. számú melléklet

Programnyilvántartás

Program azonosító	Program készítő neve	Program megnevezése	Megjegyzés
001	Magyar Államkincstár	Központosított Illetmény-számfejtési Rendszert KIRA munkaügyi intézményi modulja	
002	Andit Solutions Kft. Guethné Horváth Andrea	AndiT - Tárgyieszköz analitikus nyilvántartó program –	
003	Korend Rendszerház Kft (2800 Tatabánya, Mártírok útja 12. 3/3, Telefon/fax: +3634 309-021, mobil: +3620 220 3419, Adószám: 13666387-2-11, Cégjegyzék száma: 11-09-011392)	GORDIUS Pénzügyi Információs Rendszer és FŐKA (főkönyvi könyvelés) modulja	
004	Magyar Államkincstár	Költségvetés Gazdálkodási Rendszer K11 KTR almodulja	
005	Unicredit Bank	Spectra ügyfélterminál program	

5. számú melléklet

006	Naturasoft Magyarország Kft.	Naturasoft Raktárstart, raktári anyagnyilvántartó program	
007	Yami Bt. – Gáspár Csaba - programfejlesztő (8638 Balatonlelle, Szélső u. 9., mobil: +36 30 990-8336)	Óvodai adatbázisok: Menzasoft III étkezés-nyilvántartó, számlázó program Iskolai-kollégiumi adatbázisok: MENZA MS étkezés-nyilvántartó, számlázó program	
008	Microsoft	Bitlocker alkalmazás	
009	AC Soft Kft. (Székesfehérvár, Géza u. 32.)	IRMA iktatórendszer	
010	**Sicontact Kft.** H-1106 Budapest, Örs vezér tere 25/C Árkád Irodaház 4. emelet Tel.: +36-1-346-7052 Fax: +36-1-999-7977 E-mail: info@sicontact.hu	ESET NOD32 vírusvédelmi és biztonsági szoftver	

6. számú melléklet

Gordius jogosultságok

Szervezeti egység	***Név***	***Beosztás***	***Jogosultságok***		
			18 óvoda	***GAMESZ***	***GAMESZ gyakorló***
Igazgató	Imréné Erényi Katalin	Igazgató	X	X	X
Gazdasági Igazgatóhelyettes	Boros Tünde	Gazdasági Igazgatóhelyettes	X	X	X
Igazgatóhelyettes	Sebestyénné Pethő Andrea	Igazgatóhelyettes	X	X	X
Belső ellenőrzés	Krizmanich Henrietta	Belsőellenőrzési vezető	X	X	X
Étkeztetési csoport	Pegán Orsolya	Étkeztetési csoportvezető	Szamóca modul - Kis Gordius		
Anyaggazdálkodási csoport	Némethné Szigetvári Dóra	Anyaggazdálkodási csoportvezető	X	X	X
Anyaggazdálkodási csoport	Bata Adrienn	Gazdasági előadó	X	X	X
Személyügyi csoport	Kovács Miklósné	Személyügyi csoportvezető	X	X	X
	Törökné Kánya Nikoletta	Személyügyi ügyintéző	X	X	X
	Baranyai Katalin	Személyügyi ügyintéző	X	X	X
	Kulcsár Luca	Személyügyi ügyintéző	X	X	X
	Dávid Ildikó	Gazdasági ügyintéző	X	X	X
Pénzügyi és könyvelési csoport	Tánczosné Hédi Krisztina	Pénzügyi és könyvelési csoportvezető	X	X	X
	Zelles-Török Lívia	Gazdasági főelőadó	X	X	X
	Tóth Adrienn	Gazdasági ügyintéző	X	X	X
	Derdák Tamásné	Könyvelő	X	X	X
	Kiss Hermina Ibolya	Gazdasági ügyintéző	X	X	X
	Visnyovszky Lászlóné	Gazdasági ügyintéző	X	X	X
	Jákli Magdolna	Gazdasági ügyintéző	X	X	X
	Szilvágyi Andrea	Gazdasági ügyintéző	X	X	X

Engedélyezők:

Imréné Erényi Katalin
Igazgató

Sebestyénné Pethő Andrea
Igazgatóhelyettes

Boros Tünde
Gazdasági igazgatóhelyettes

7.számú melléklet
Irma érkeztetési jogosultságok

IRMA SZÁMLA ÉRKEZTETÉSI jogosultságok

Érkeztetőkönyv	Telephely (Szombathely)	Szervezeti egység	Érkeztetők (írási - módosítási jog)	Betekintők (olvasási jog)
"évszám"	Boglárka u. 2 Nádasdy F. u. 4.	SZOMBATHELYI KÖZNEVELÉSI GAMESZ	Dávid Ildikó Sziklai Amanda Törökné Kánya Nikoletta Kiss Hermina Ibolya	Boros Tünde Tánczosné Hédi Krisztina Pegán Orsolya Bata Adrienn

Engedélyezők:

.....
Imréné Erényi Katalin
igazgató

.....
Sebestyénné Pethő Andrea
igazgatóhelyettes

.....
Boros Tünde
gazdasági igazgatóhelyettes

8. melléklet

IRMA iktatórendszer jogosultságok

Iktatókönyv	Telephely (Szombathely)	Szervezeti egység	Iktatószámok sávos kiosztása	Iktató	Ügyintéző	Betekintő
Igazgato "évszám"	Boglárka u.	Igazgató	1001-1999	Sziklai Amanda Kiss Hermina Ibolya Szilvágyi Andrea Dávid Ildikó Némethné SzigetváriDóra Kovács Anita Bata Adrienn	Imréné Erényi Katalin	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta
Ellenorzes "évszám"		Belső ellenőrzés	2001-2499	Szilvágyi Andrea Kiss Hermina Ibolya	Sebestyénné Pethő Andrea Krizmanich Henrietta	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta
OvEll "évszám"		Élelmezési csoport	2500-2999	Dávid Ildikó Prikazovics Judit Sziklai Amanda	-	Imréné Erényi Katalin Sebestyénné Pethő Andrea Boros Tünde Pegán Orsolya Krizmanich Henrietta Dávid Ildikó
Munkaugy "évszám"		Humánerőforrás- és bérügyi csoport	3001-3999	Szilvágyi Andrea Kiss Hermina Ibolya	Kovács Miklósné Baranyai Katalin	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta Kovács Miklósné
Gazdasagi "évszám"		Gazdasági igazgatóhelyettes és Pénzügyi és könyvelési csoport	4001-4999	Szilvágyi Andrea Kiss Hermina Ibolya	Boros Tünde Tánczosné Hédi Krisztina Tóth Adrienn Szilvágyi Andrea Zelles-Török Lívia Derdák Tamásné	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta Dávid Ildikó Tánczosné Hédi Krisztina Boros Tünde
Ig.helyett "évszám"	Nádasdy F. u. 4.	Igazgató helyettes	5001-5999	Sziklai Amanda Dávid Ildikó Bata Adrienn Kovács Anita Némethné Szigetvári Dóra	Sebestyénné Pethő Andrea	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta Kovács Anita Némethné Szigetvári Dóra Bata Adrienn
Muszaki "évszám"		Karbantartási csoport Informatikai csoport	6001-6999	Sziklai Amanda Dávid Ildikó Kovács Anita Bata Adrienn Némethné Szigetvári Dóra	Sebestyénné Pethő Andrea Sisak József Sifter József Szandi Zoltán Némethné Szigetvári Dóra Kovács Anita Szucsányi Bata Adrienn	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta Sisak József Kovács Anita Némethné Szigetvári Dóra Dávid Ildikó Bata Adrienn Boros Tünde
Vagyon (Anyag)"évszám"		Anyaggazdálkodási csoport, Beszerzés	7001-7999	Sziklai Amanda Dávid Ildikó Kovács Anita Bata Adrienn Némethné Szigetvári Dóra	Sebestyénné Pethő Andrea Némethné Szigetvári Dóra Sisak József Szandi Zoltán Sifter József Kovács Anita Bata Adrienn	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta Némethné Szigetvári Dóra Dávid Ildikó Sisak József Kovács Anita Bata Adrienn
Elelm "évszám"		Élelmezési csoport	8001-8999	Pegán Orsolya Hajnal Kornélia Prikazovics Judit	Pegán Orsolya Hajnal Kornélia Prikazovics Judit	Imréné Erényi Katalin Sebestyénné Pethő Andrea Krizmanich Henrietta Dávid Ildikó Boros Tünde

Imréné Erényi Katalin

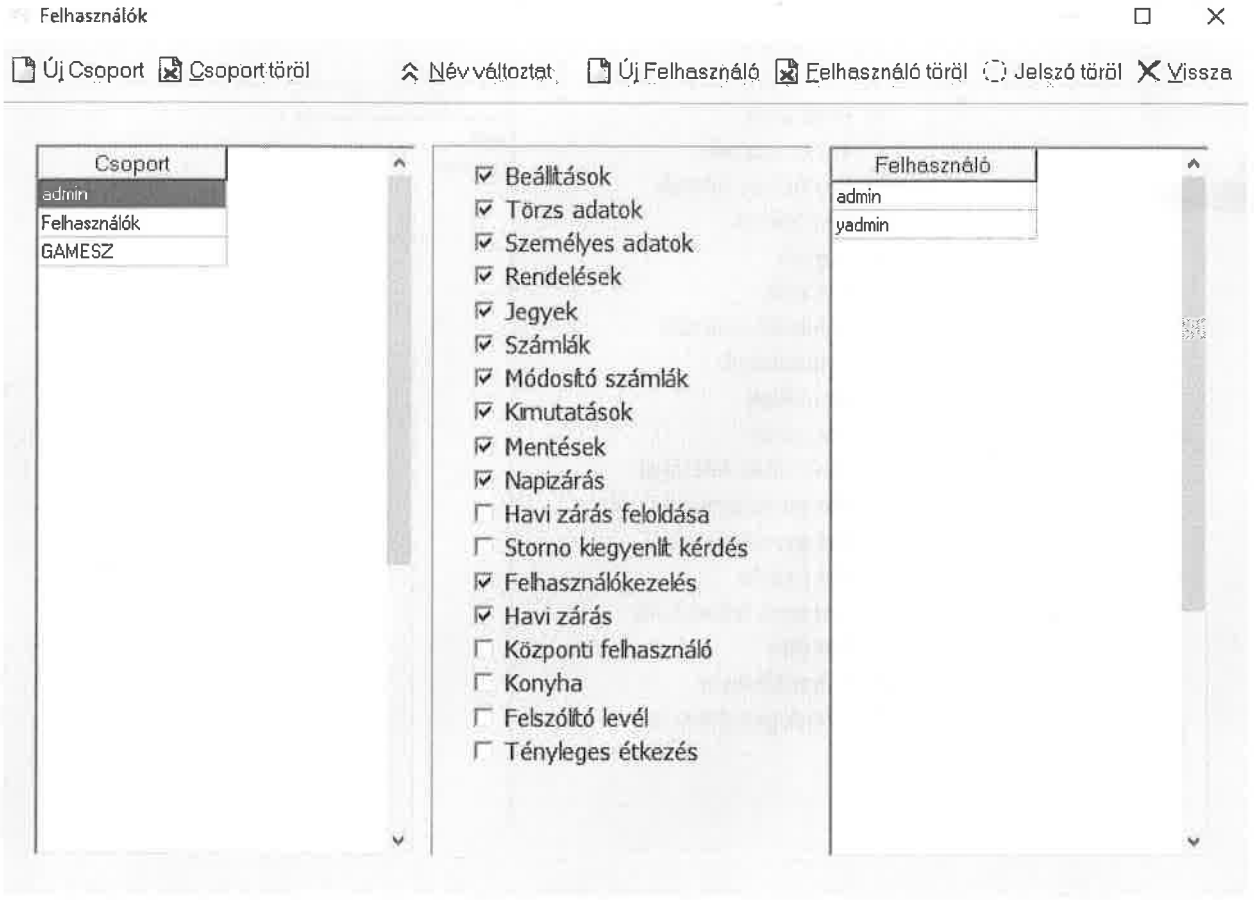
Sebestyénné Pethő Andrea

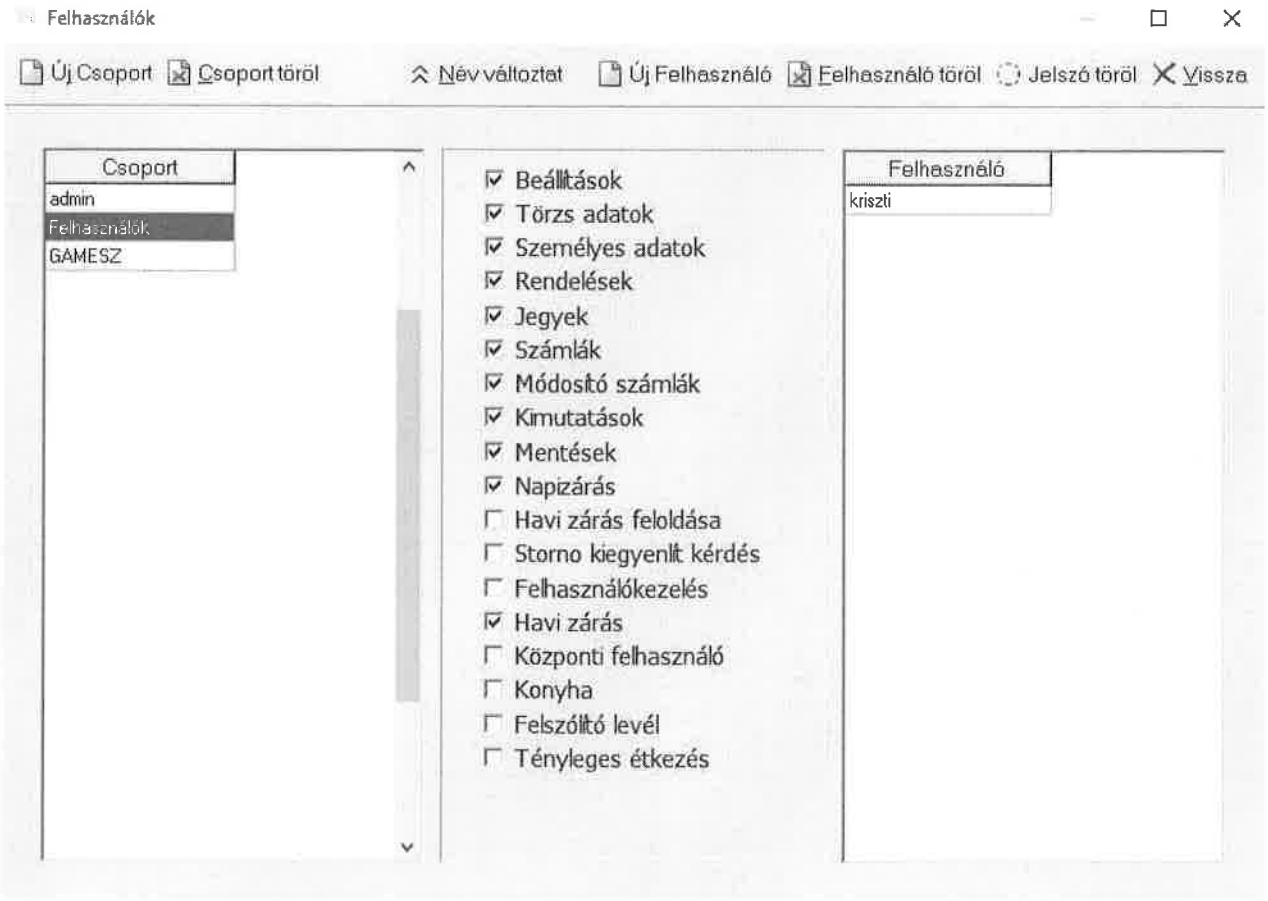
Boros Tünde

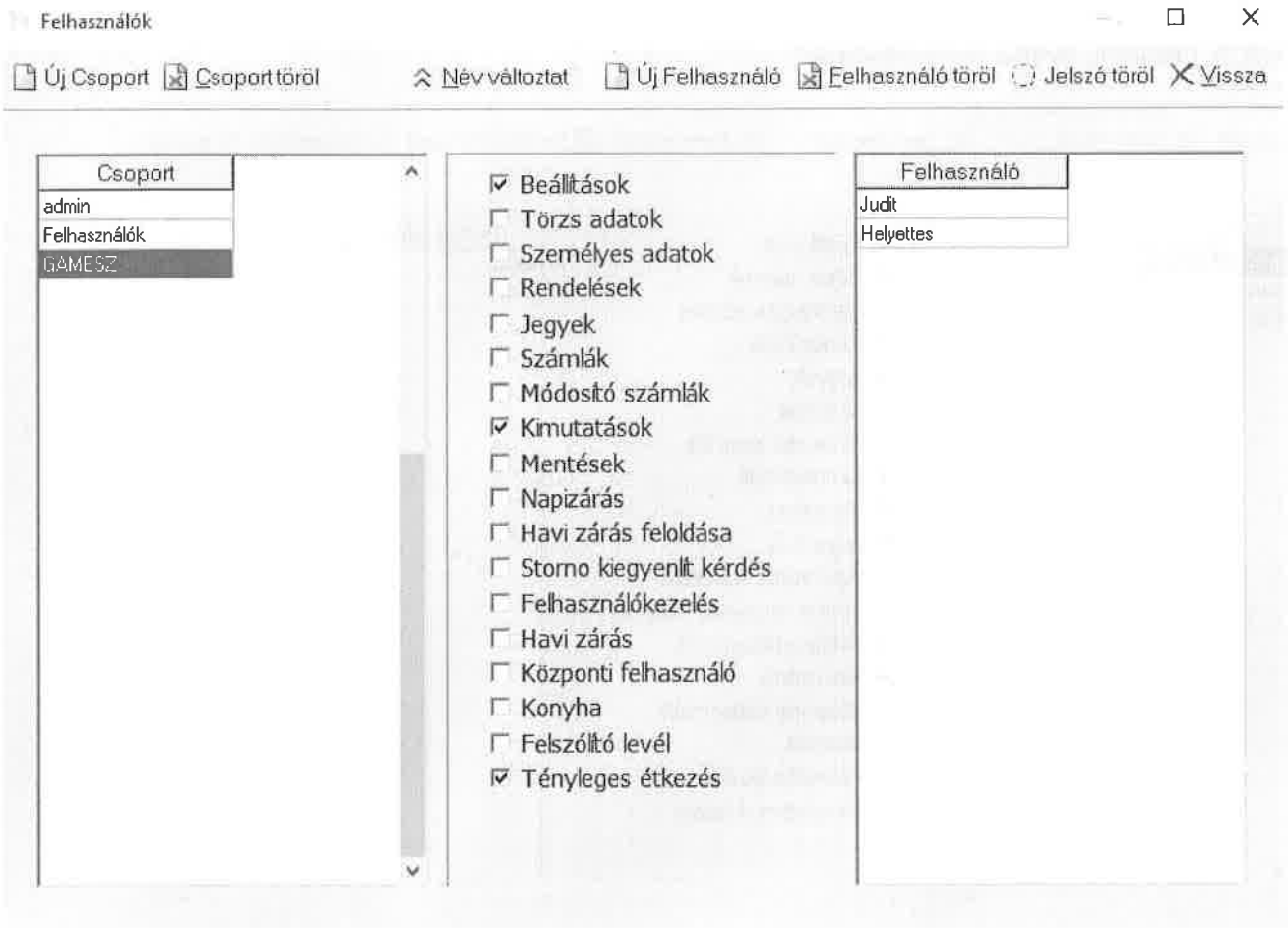
igazgató	igazgatóhelyettes	gazdasági igazgatóhelyettes
	X	

9. melléklet

MenzaSzoft III. program, óvodai jogosultságok:






Felhasználók
Új Csoport
Csoport töröl
Névváltoztat
Új Felhasználó
Felhasználó töröl
Jelszó töröl
Vissza
Csoport
admin
Felhasználók
GAMESZ
Beállítások
Törzs adatok
Személyes adatok
Rendelések
Jegyek
Számlák
Módosító számlák
Kimutatások
Mentések
Napizárás
Havi zárás feloldása
Storno kiegyenlít kérdés
Felhasználókezelés
Havi zárás
Központi felhasználó
Konyha
Felszólító levél
Tényleges étkezés
Felhasználó
Judit
Helyettes

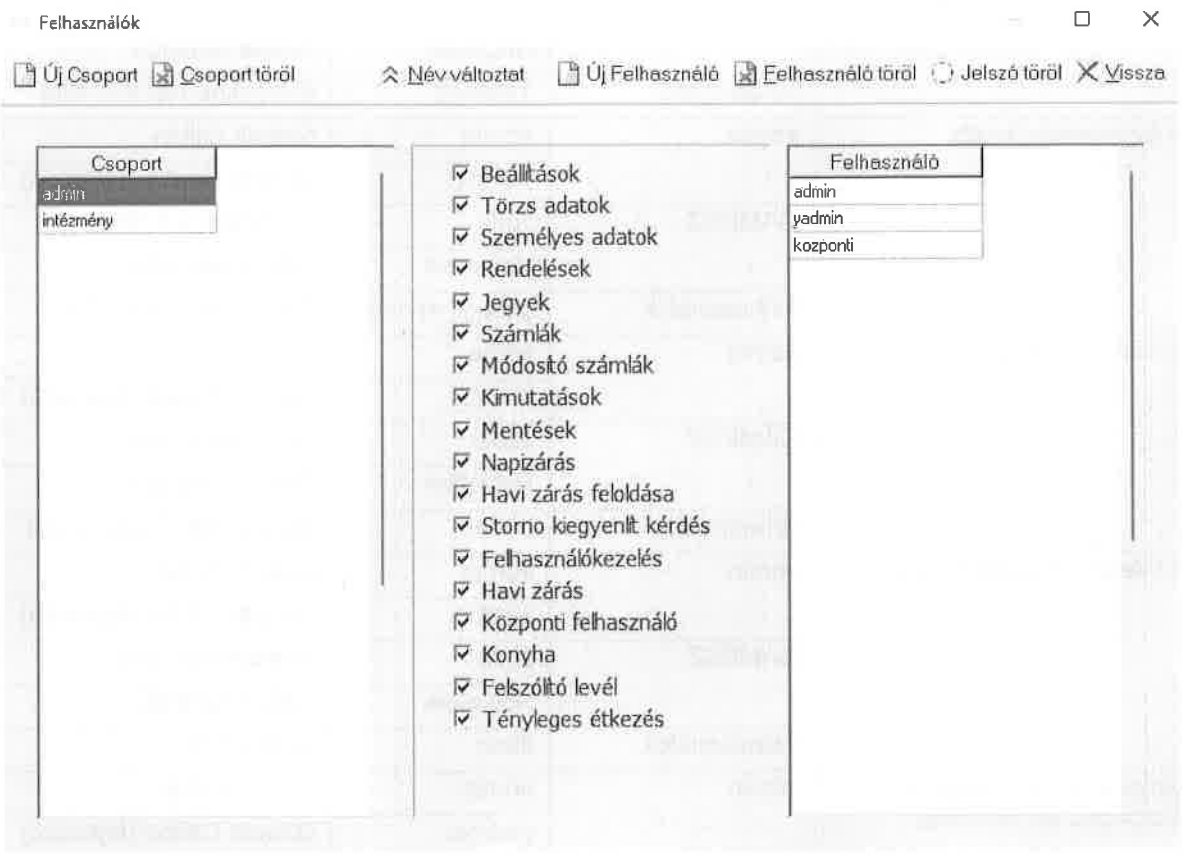
Óvodai jogosultsági csoportok			
Intézmény	***Jogosultsági csoport***	***USER***	***Felhasználó neve***
Szombathelyi Aréna Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	kriszti	Dömötörné Dávid Krisztina
Szombathelyi Barátság Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	baratsag	Sütő Péterné
Szombathelyi Benczúr Gyula Utcai Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Titkár	Tömőné Nardai Anita
Szombathelyi Donászy Magda Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Titkar	Kovács Tiborné
Szombathelyi Gazdag Erzsi Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	pankasza	Pankasz Andrea
Szombathelyi Hétszínvirág Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Titkarno	Horváthné Bálint Éva

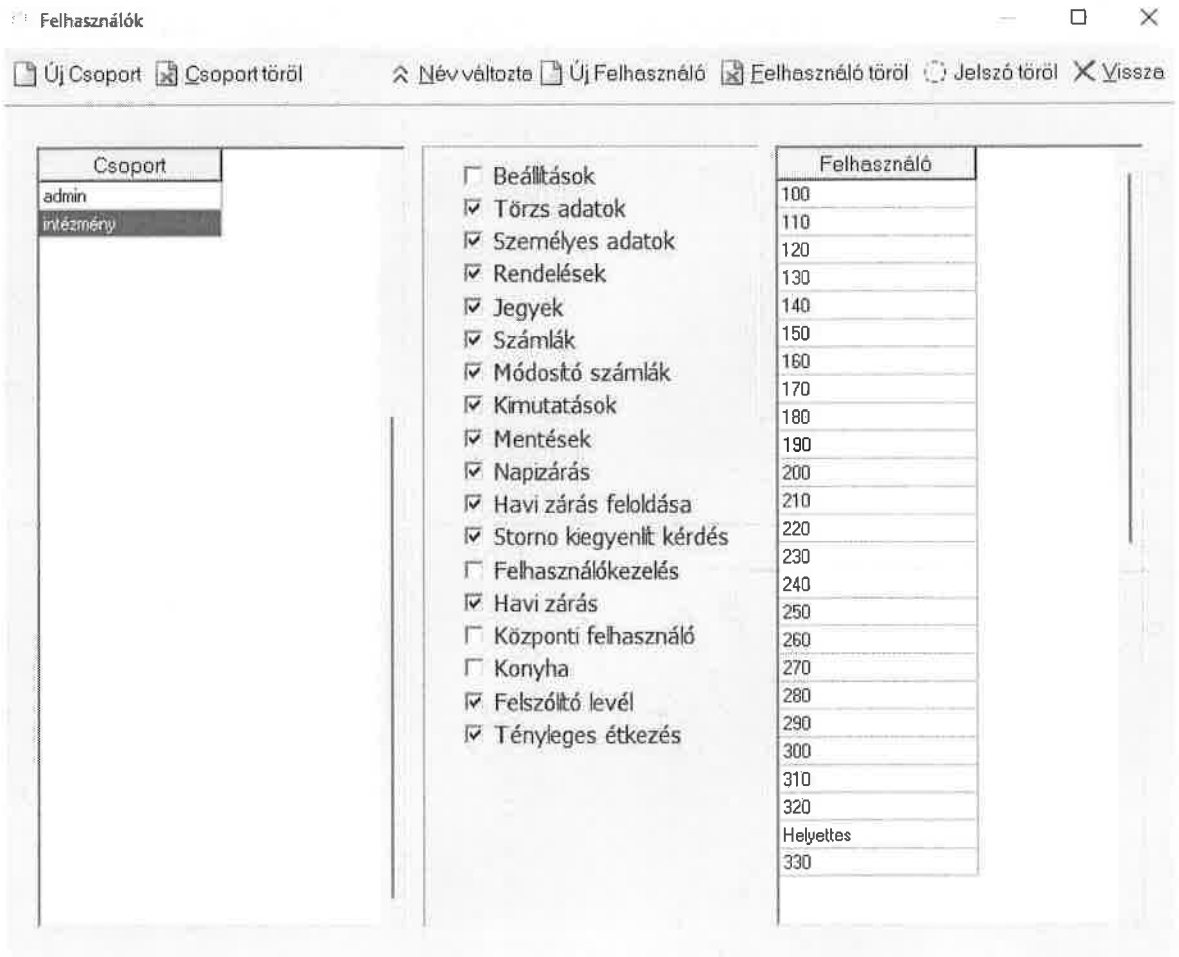
Szombathelyi Játéksziget Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	jateksziget	Márkus - Rákli Veronika
Szombathelyi Kőrösi Csoma Sándor utcai Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	Aniko	Borbás Anikó
Szombathelyi Margaréta Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	titkar	Csonkáné Farkas Anita
Szombathelyi Maros Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	rakli.anna	Rákli Annamária
Szombathelyi Mesevár Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Titkár	Miszinė Tancsics Barbara
Szombathelyi Mocorgó Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Titkár	Barczáné Molnár Rita
Szombathelyi Napsugár Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	Napsugárovoda	Kozma-Kormos Adél
Szombathelyi Pipitér Óvoda - Farberkamille Kindergarten Steinamanger	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	Pipiterovi	Gyöngyössyné Andrea
		Pedasszisztens	Sthauerné Tóth Ramóna

Szombathelyi Szivárvány Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Titkárnő	Bendákné Németh Rita
Szombathelyi Szűrcsapó Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	gaspar.istvanne	Gáspár Istvánné (Ági)
Szombathelyi Vadvirág Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	felhasznalo	Erika	Szilvágyiné Szalay Erika
Szombathelyi Weöres Sándor Óvoda	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Judit	Prikazovics Judit
		Helyettes	Sziklai Amanda
	Felhasználók	titkar	Szölke Edit
Aranyhíd Egységes Gyógypedagógiai, Konduktív Pedagógiai Módszertani Intézmény Micimackó Óvodája	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
	GAMESZ	Helyettes	Sziklai Amanda
	Felhasználók	cstimi	Csigó Tímea

10. melléklet

MenzaSzoft III., MENZA MS program iskolai jogosultságok





iskolai jogosultsági csoportok			
Intézmény	***Jogosultsági csoport***	***USER***	***Felhasználó neve***
Szombathelyi Bercsényi Miklós Általános Iskola	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		kozponti	Pegán Orsolya
	intézmény	160	Gőcze Gáborné
		Helyettes	Étkezési csoportvezető határozza meg
Szombathelyi Derkovits Gyula Általános Iskola	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		kozponti	Pegán Orsolya
	intézmény	190	Tóth Tiborné
		Helyettes	Étkezési csoportvezető határozza meg
Szombathelyi Neumann János Általános Iskola	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		kozponti	Pegán Orsolya
	intézmény	260	Tóth Tiborné
		Helyettes	Étkezési csoportvezető határozza meg
Szombathelyi Paragvári Utcai Általános Iskola	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	180	Nagy Marietta
		Helyettes	Étkezési csoportvezető határozza meg
Szombathelyi Dési Huber István Általános Iskola	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	170	Nagy Marietta
		Helyettes	Étkezési csoportvezető határozza meg

Szombathelyi Váci Mihály Általános Iskola	admin	admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	130	Hajnal Kornélia
		Helyettes	Étkezési csoportvezető határozza meg
Oladi Általános Iskola	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	150	Éder Tíborné
		Helyettes	Étkezési csoportvezető határozza meg
Nyitra Utcai Általános Iskola	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	300	Szilvágyiné Szalay Erika
		Helyettes	Étkezési csoportvezető határozza meg
Gothard Jenő Általános Iskola	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	200	Gőcze Gáborné
		Helyettes	Étkezési csoportvezető határozza meg
Szombathelyi Zrínyi Ilona Általános Iskola	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	270	Kárer Barbara
		Helyettes	Étkezési csoportvezető határozza meg
Kanizsai Dorottya Gimnázium	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	210	Éder Tíborné
		Helyettes	Étkezési csoportvezető határozza meg
Németh Pál Kollégium	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	230	Éder Tíborné
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum **Horváth Boldizsár** Közgazdasági és Informatikai Technikum	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	320	Kárer Barbara
		Helyettes	Étkezési csoportvezető határozza meg

Vas Megyei Szakképzési Centrum Kereskedelmi és Vendéglátó Technikum	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	240	Hajnal Kornélia
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum Kereskedelmi és Vendéglátó **Kollégium**	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	250	Hajnal Kornélia
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum **Puskás** Tivadar Szakképző Iskola és Kollégium	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	310	Hajnal Kornélia
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum **Gépipari** és Informatikai Technikum	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	290	Hajnal Kornélia
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum **Savaria** Technikum	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	120	Prikazovics Judit
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum Hollán Ernő Kollégium	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	110	Prikazovics Judit
		Helyettes	Étkezési csoportvezető határozza meg
Berzsenyi Dániel Kollégium	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	280	Hajnal Kornélia
		Helyettes	Étkezési csoportvezető határozza meg
Nagy Lajos Gimnázium	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	100	Pegán Orsolya
		Helyettes	Étkezési csoportvezető határozza meg

Szombathelyi Művészeti Szakgimnázium és Technikum	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	220	Kárer Barbara
		Helyettes	Étkezési csoportvezető határozza meg
Aranyhíd Egységes Gyógypedagógiai, Konduktív Pedagógiai Módszertani Intézmény	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	140	Sziklai Amanda
		Helyettes	Étkezési csoportvezető határozza meg
Vas Megyei Szakképzési Centrum **Hefele** Menyhért Szakképző Iskola	admin	Admin	Szandi Zoltán
		yadmin	Gáspár Csaba (fejlesztő)
		Központi	Pegán Orsolya
	intézmény	330	Gőcze Gáborné
		Helyettes	Étkezési csoportvezető határozza meg