A Prizma Általános Intézmény és Óvoda, Egységes Gyógypedagógiai Módszertani Intézmény (1134 Budapest, Váci út 57.) informatikai biztonsági Szabályzata

Verzió: 2.0

Hatályba lépés időpontja: 2017.

Jóváhagyta: Németh Ildikó intézményvezető

Tartalomjegyzék:

1. Bevezetés ... 3
2. Fogalmak meghatározása ... 3
3. A szabályzat jogszabályi háttere ... 5
4. A szabályzat területi, személyi és időbeli hatálya, módosítása ... 5
5. A szabályzat célja ... 5
6. A kerületi Informatikai Szolgáltató Osztály ... 6
7. Az intézményi informatikai felügyeletet ellátó személy ... 6
8. Az intézményi felhasználói jogok, kötelességek, tilalmak és szankciók ... 6
9. Az informatikai infrastruktúra működési rendje ... 7
9.1. Az informatikai infrastuktúra használatára vonatkozó rendelkezések ... 7
9.2. Az informatikai hálózat használatára vonatkozó tilalmak ... 8
9.3. Az informatikai hálózat használati szabályai megsértésének szankciói ... 8
10. Az informatikai eszközök használatának rendje ... 9
10.1. A szerver működtetésének, használatának rendje ... 9
10.2. A munkaállomások használatának rendje ... 9
10.3. A számítástechnika terem használatának rendje ... 9
11. A szoftverek használatának rendje ... 10
11.1. A szoftverekkel kapcsolatos általános rendelkezések ... 10
11.2. A szoftverek telepítése, használata ... 10
12. A számítástechnikai adathordozók használatának rendje ... 10
12.1. Az intézményi adathordozók tárolása, használata és karbantartása ... 10
12.2. Az adathordozók nyilvántartása és megőrzése ... 11
12.3. Az adathordozók selejtezése ... 11
13. Az elektronikus nyilvántartások ... 11
14. Elektronikus szolgáltatások ... 12
14.1. Az adatszolgáltatás általános szabályai ... 12
14.2. Az elektronikus levelezés ... 12
14.3. Az intézmény honlapja ... 13
15. Záró rendelkezések ... 13
16. A szabályzat mellékletei ... 14

1. Bevezetés

Az informatikai rendszerek és eszközök mindennapos használata szükségessé teszi az információbiztonsággal kapcsolatos elvek, szabályok, elvárt és betartandó magatartásformák és gyakorlat meghatározását. Ezért a Prizma Általános Iskola és Óvoda, Egységes Gyógypedagógiai Módszertani Intézmény alkalmazotti testülete a következő Informatikai Biztonsági Szabályzatot fogadta el.
Az Informatikai Biztonsági Szabályzat egy olyan belső szervezeti intézkedés, amely az intézményben működtetett informatikai rendszerekre vonatkozóan szabályozza az informatikai rendszerrel kapcsolatos biztonsági intézkedéseket, szervesen illeszkedve a szervezet egyéb működési és ügyrendi előírásaihoz (Szervezeti és Működési Szabályzat és mellékletei).

2. Fogalmak meghatározása

Informatikai infrastruktúra: az intézményhez kapcsolódó feladatokat ellátó, illetve az intézményi hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese.

Rendszergazda: az informatikai infrastruktúra hardver- és szoftverelemeinek, valamint szolgáltatásainak működését technikailag biztosító felelős.

Üzemeltető: az adott szoftver-, vagy hardverelemet az intézmény nevében üzembe állító és üzemeltető rendszergazda.

Felhasználó: az a személy, aki az intézmény informatikai infrastruktúrájának vagy szolgáltatásainak valamely elemét igénybe veszi.

Intézményi felhasználó: olyan felhasználó, aki az intézménnyel munkavállalói jogviszonyban van.

Informatikai szolgáltatás: az informatikai infrastruktúra olyan részhalmaza, amely az intézményi felhasználó számára meghatározott funkcionalitást nyújt.

Publikus szolgáltatás: olyan szolgáltatás, amelyet az intézményi felhasználókon kívül mások is – korlátozottan vagy korlátozás nélkül – igénybe vehetnek.

Szerver: olyan feladatokat ellátó számítógép, amely az intézményi hálózatra kapcsolódik és felhasználói köre számára szolgáltatást nyújt.

Munkaállomás: az intézményi hálózathoz kapcsolt olyan számítógép, amely nem tekinthető szervernek és egyértelműen valamely intézményi felhasználóhoz vagy intézményi felhasználói csoporthoz rendelhető.

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.

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.

Informatikai biztonság: Az informatikai biztonság az az állapot, amikor az informatikai rendszer által kezelt adatok védelme — bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából — zárt, teljes körű, a kockázatokkal arányos és folyamatos. Az informatikai biztonság két alapterülete az információvédelem és a megbízható működés.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen.

Megbízható működés: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a rendelkezésre állás, és a funkcionalitás sérülése, elvesztése ellen.

3. A szabályzat jogszabályi háttere

- A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló többször módosított 1992. évi LXIII. törvény
- A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény
- A szerői jogról szóló 1999. évi LXXVI. törvény
- A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben
- Az állami- és szolgálati titokról szóló 1987. évi 5. sz. törvényerejű rendelet
- Az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés
- 2013. évi CCXLV. törvény

4. A szabályzat területi, személyi és időbeli hatálya, módosítása

Az Informatikai Biztonsági Szabályzat területi hatálya kiterjed:

- az intézményben védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- az intézmény tulajdonában lévő valamennyi informatikai berendezésre,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

Jelen szabályzat a Prizma Általános Intézmény és Óvoda, Egységes Gyógypedagógiai Módszertani Intézmény alkalmazottaira illetve az intézményi informatikai infrastruktúra más felhasználóira egyaránt vonatkozik.

Jelen szabályzat **2017. ….. -tól** visszavonásig érvényes. Egyúttal érvényét veszti az intézmény korábbi Számítástechnikai védelmi szabályzata.

A szabályzatot a törvényi, jogi szabályozásoknak megfelelően illetve az informatika fejlődése során bekövetkező változásoknak megfelelően kell felülvizsgálni, módosítani.

5. A szabályzat célja

Az intézményi Informatikai Biztonsági Szabályzat célja:

- a titok-, vagyon - és tűzvédelemre vonatkozó védelmi intézkedések meghatározása;
- az üzemeltetett számítógépek, valamint azok kiegészítő eszközeinek rendeltetésszerű használata szabályainak meghatározása;
- az üzembiztonságot szolgáló karbantartás és fenntartás feladatainak előírása;
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése;
- a személyes adatok védelme és a közérdekű adatok nyilvánosságának biztosítása;
- az adatállományok tartalmi és formai épsége megőrzésének, valamint az adatállományok biztonságos mentésének elősegítése.

6. A kerületi Informatikai Szolgáltató Osztály

A XIII. kerüli Önkormányzat Informatikai Szolgáltató Osztálya (továbbiakban: ISZO) a KLIK fenntartásában működő közoktatási intézményekben az alábbi feladatokat látja el:

- Az internetszolgáltatás hibáinak jelzése a szolgáltató felé.
- Az Önkormányzat tulajdonában lévő, az intézménybe kihelyezett hálózati eszközök felügyelete, menedzselése.

7. Az intézményi informatikai felügyeletet ellátó személy

Az intézményi informatikai felügyeletet ellátó munkatárs az intézmény szervezetébe tartozó személy.

Feladatai:

- az intézményi informatikai infrastruktúra üzemeltetése, szükség szerinti fejlesztése;
- az intézmény szervezeti egységei informatikai eszközeinek, adatbázisainak, szoftvereinek szolgáltatásainak üzemeltetése;
- az informatikai eszközbeszerzések koordinálása, ezzel kapcsolatos szaktanácsadás;
- informatikai tanácsadás, tájékoztatás.

Az intézményi informatikai felügyeletet ellátó munkatárs bármikor jogosult az informatikai infrastruktúra szabályos használatát, működését ellenőrizni és az információkat csak elektronikus formában szolgáltatni mindazok számára, akik hozzáférnek az informatikai infrastruktúrához.

Kötelessége a károkat megelőzni, illetve a bekövetkezett károk következményeit mérsékelni, felszámolni; illetve titokban tartani a nagyobb jogosultsági köréből eredően birtokába jutott személyes vagy bizalmas információkat.

Az intézményi informatikai felügyeletet ellátó munkatársnak tilos a nagyobb jogosultsági körével visszaélni, azt a számára kijelölt feladatkörön kívül felhasználni; illetve tilos továbbadni a nagyobb jogosultsági köréből eredően birtokába jutott személyes vagy bizalmas, illetve titokkörbe tartozó adatokat.

8. Az intézményi felhasználói jogok, kötelességek, tilalmak és szankciók

Valamennyi intézményi felhasználónak joga van:

- az intézmény informatikai infrastruktúrájának a használatához;
- tájékoztatást kapni a felhasználói szabályokról, az informatikai infrastruktúrával kapcsolatos feladat- és hatáskörökről;
- tanulmányaikhoz, feladataik elvégzéséhez szükséges közhasznú információkhoz jutni.

Valamennyi intézményi felhasználó kötelessége:

- rendeltetésszerűen használni az intézmény informatika infrastruktúráját;
- tájékozódni a felhasználási szabályokról;
- titokban tartani az intézmény informatikai infrastruktúrájának igénybevételéhez biztosított azonosítókat;

- tájékoztatni az informatikai felügyeletet ellátó személyt a működési hibákról, a nem rendeltetésszerű vagy törvénytelen használatról;
- együttműködni és segíteni az informatikai felügyeletet ellátó személyt vagy nyomozó hatóságot a működési hibák, nem rendeltetésszerű vagy törvénytelen használat felderítésére indult vizsgálatban.

Valamennyi intézményi felhasználónak tilos

- olyan jogosultságok megszerzése illetve megszerzésére kísérletet tenni, amely a felhasználó számára nem engedélyezett;
- a biztonsági rendszerek feltörése, illetve annak kísérlete;
- másoknak jogosultságok átadása;
- szoftver, hardver elemek megrongálása, működésük veszélyeztetése;
- szoftver, hardver elemek jogosulatlan módosítása, átkonfigurálása;
- meghibásodás esetén a hiba elhárításának jogosulatlan megkezdése;
- a hálózati forgalom figyelése, adatok gyűjtése.

Az intézményi felhasználói tilalmak megszegése esetén az intézményi felhasználó a nem rendeltetésszerű vagy törvénytelen használatból eredő károkért jogi és kártérítési felelősséggel tartozik. A szabályok ismeretének hiánya nem mentesít a szankciók illetve a jogi és kártérítési felelősség alól.

A szabályok be nem tartása esetén az informatikai felügyeletet ellátó személy a felhasználó hozzáférési jogát korlátozhatja, bűncselekmény elkövetése esetén pedig azonnali hatállyal minden hozzáférési jogot megvon és értesíti a hatóságokat.

9. Az informatikai infrastruktúra működési rendje

9.1. Az informatikai infrastuktúra használatára vonatkozó rendelkezések

- Az informatikai infrastruktúra valamennyi hálózati aktív és passzív eleme a fenntartó illetve az intézmény tulajdona.
- A hálózat célja önkormányzati, országos és nemzetközi számítógépes hálózati kapcsolatok és információs szolgáltatások biztosítása a felhasználói kör részére oktatási, tudományos és hivatali célokra. A hálózatot a felhasználók a fenti célokra használhatják. Ebbe beleértendő a hálózatnak az intézmény alaptevékenységéhez kapcsolódó adminisztratív és információs feladataival összefüggő célokra történő használata is. Korlátozott mértékben megengedett a hálózat magáncélra (pl. magánjellegű levelezés) történő felhasználása, de ez nem jelenthet üzleti célú felhasználást. Aki a hálózaton keresztül más hálózatba átlép (Pl. Internet), idegen szolgáltatót vesz igénybe, az idegen hálózatra érvényes szabályokat is köteles betartani.
- Az intézményi felhasználó saját tulajdonú hálózati aktív vagy passzív elemet az informatikai infrastruktúrához csak a rendszergazda engedélyével kapcsolhat.
- Az informatikai infrastruktúrában routert (útválasztó) vagy router funkciókat ellátó számítástechnikai eszközt kizárólag a rendszergazda állíthat, vagy állíttathat üzembe.
- A felhasználók személyesen felelnek az általuk generált hálózati forgalomért.
- A használati szabályok betartatása a hálózati menedzser feladata. A dinamikusan kiosztott címek esetén (pl. DHCP) a címtartományért a címszolgáltató gép

üzemeltetője felelős, és ő köteles a címek kiosztását naplózni, és a kapcsolódó felhasználói fizikai címeket nyilvántartani. Közös használatú számítógépek esetén (hallgatói laborok, tanári szobák stb.) a számítógépet igénybe vevő személyek jogosultságát ellenőrizni kell.

9.2. Az informatikai hálózat használatára vonatkozó tilalmak

A hálózat nem használható az alábbi tevékenységekre, illetve az ilyen tevékenységekre irányuló próbálkozásokra, kísérletekre:

- Az érvényes magyar törvényekbe ütköző cselekmények, ideértve a következőket, de nem korlátozódva ezekre: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos és tudatos illegális terjesztése.
- A más fenntartóhoz tartozó intézmények egymás közötti átmenő forgalmának bonyolítása.
- Az önkormányzat hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik.
- A hálózat szolgáltatásainak nem tankerületi intézmények, felhasználók számára való továbbítása.
- Profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése.
- A hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység, ilyen információk, programok terjesztése.
- A hálózatot, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybe vevő tevékenység (pl. levélbombák, hálózati játékok), a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása.
- A hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére irányuló tevékenység.
- Másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf, pedofil anyagok közzététele).
- Mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása (pl. kéretlen levelek, hirdetések).
- A hálózati erőforrások magáncélra való túlzott mértékű használata, a hálózati erőforrásoknak, szolgáltatásoknak olyan célra való használata, amely az erőforrás/szolgáltatás eredeti céljától idegen (pl. hírcsoportokba/levelezési listákra a csoport/lista témájába nem vágó üzenet küldése).
- A hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről, vagy más felhasználótól származna (spoofing).

9.3. Az informatikai hálózat használati szabályai megsértésének szankciói

Az informatikai hálózat használati szabályai megsértésének gyanúja esetén, a rendszergazda és a Tankerület illetékes képviselője az adott eseményt kivizsgálja. A szabályzat szándékos és durva megsértésének szankcionálása a hálózati szolgáltatásokból való azonnali ideiglenes kizárás. Ha a szabálysértés kismértékű, vagy nem tekinthető szándékosnak, akkor az elkövetőt figyelmeztetni, és a szabályokról tájékoztatni kell. A figyelmeztetés utáni ismételt elkövetést szándékosnak kell tekinteni. Szükség esetén a Tankerület jogi felelősségre vonást kezdeményezhet a szervezeti egység vezetőjénél.

Az ISZO hálózati menedzsment a nagyobb károkozás elkerülése végett az érintett alhálózat forgalmát korlátozhatja, vagy szüneteltetheti. A szabályokat megsértő személy címének ismeretében az ISZO a megadott cím részleges vagy teljes szűrését is elvégezheti.

Az ISZO saját hatáskörében a hálózat forgalmát célszerűen szabályozó további intézkedéseket vezethet be, melyek meghirdetésre kerülnek. Ezek betartása kötelező.

10. Az informatikai eszközök használatának rendje

10.1. A szerver működtetésének, használatának rendje

A szervernek műszakilag alkalmasnak kell lennie a tervezett szolgáltatás nyújtására. A szervereket, illetve az általuk nyújtott szolgáltatások stabil, biztonságos üzemeltetése érdekében, gépteremben kell elhelyezni. A gépteremre az alábbi szabályok vonatkoznak:

- a gépterem biztonsági zárakkal felszerelt;
- a terembe csak arra jogosult személyek juthatnak be;
- a teremben tilos a dohányzás, étel és ital tárolása, fogyasztása;
- a portaszolgálat ismeri a terem áramtalanításának, a tűz oltásának módját;
- takarító személyzet csak felügyelet mellett tartózkodik, végzi munkáját a teremben.

10.2. A munkaállomások használatának rendje

- A munkaállomások beszerzését a Tankerület végzi. Az első üzembe helyezést és az informatikai infrastruktúrához való csatlakoztatást az intézmény rendszergazdája végzi el.
- Meghibásodás esetén az intézmény rendszergazdáját kell értesíteni, aki a hibaelhárításról intézkedik.
- Az intézményi felhasználó saját tulajdonú számítógépet üzemeltethet az intézményben. A saját tulajdonú számítógépek üzemeltetési, karbantartási kötelessége a tulajdonost terheli. A saját tulajdonú számítógépen telepített szoftverek jogtisztaságáért a tulajdonos felel.

10.3. A számítástechnika terem használatának rendje

- A számítástechnika terem használatának rendjét az intézményvezető állapítja meg.
- Az eszközök csak rendeltetés szerűen használhatók, azok értékét óvni kell.
- A számítógépeken kizárólag az azokra telepített, operációs rendszer és programok használhatók.
- A gépeken lévő programok rendszerbeállítását módosítani tilos!
- A szándékosan okozott kárt a felhasználó (tanuló esetében a szülő) köteles megtéríteni.
- A terembe ételt, italt bevinni tilos.
- A teremben tanuló csak tanári felügyelettel tartózkodhat.
- A pedagógus köteles a tanulókkal ismertetni a hálózati tevékenység etikai szabályait. A számítógépes hálózatokon érvényes netikett betartása kötelező!
- Agressziót sugárzó, erotikus, bármilyen etnikai, illetve vallási meggyőződést, személyiségi jogot sértő tartalmakat nézni tilos.
- Az intézmény nem vállal felelősséget a számítógépekhez csatlakoztatott adathordozóért és annak tartalmáért.

- A tanóra végén minden pedagógus és tanuló köteles a számítógépet kikapcsolni és a helyén rendet rakni.
- A teremben található főkapcsolót tanulónak kezelni tilos!
- Munka közben az esetlegesen felmerülő számítástechnikai jellegű problémákról a pedagógust, az intézményi informatikai felügyeletet ellátó személyt tájékoztatni kell.
- A gépteremben csak engedéllyel szabad felvételt készíteni (hang, fénykép, film).

11. A szoftverek használatának rendje

11.1. A szoftverekkel kapcsolatos általános rendelkezések

- A szoftverek telepítésének, alkalmazásának a szerzői jogi törvény rendelkezéseit figyelembe véve kell történnie.
- A szoftver a létrehozók szellemi tulajdona, alkalmazásuk a rájuk vonatkozó licencszerződések feltételeinek betartásával lehetséges.
- Az intézményben tilos bárkit tudatosan vagy akaratlanul illegális szoftvermásolásra vagy felhasználásra ösztönözni, felkérni, kötelezni.
- Az intézményben tilos olyan eszközöket készíteni vagy alkalmazni, amely a szoftver védelmét szolgáló eszközök eltávolítását lehetővé teszik.
- A szoftverről biztonsági másolat készülhet, amennyiben ezt a licenc szerződés nem tiltja.
- Az intézményben vírusvédelmi és a kiskorúak biztonságos internethasználatát biztosító tartalomszűrő programot kell használni.

11.2. A szoftverek telepítése, használata

Valamennyi számítástechnikai eszközre csak jogtiszta szoftver telepíthető. A szoftverek nyilvántartása, a jogtisztaság ellenőrzése és telepítése az intézményi rendszergazda kötelessége.
Amennyiben a megvásárolt szoftvert a forgalmazó/gyártó kívánja telepíteni a telepítés csak az intézményi informatikai felügyeletet ellátó személy jelenlétében történhet.

12. A számítástechnikai adathordozók használatának rendje

12.1. Az intézményi adathordozók tárolása, használata és karbantartása

- Az adathordozók tárolása elektromos tértől és sugárzó hőtől mentes helyen történik.
- Az üres és a személyes adatokat nem tartalmazó informatikai adathordozó eszközök elhelyezése a számítástechnika teremben lévő szekrényben történik. A személyes és különleges adatokat tartalmazó adathordozók elhelyezésére zárható szekrényben kerül sor.
- Az intézményen kívüli adatforgalomban használt adathordozók előállítása, kiadása és fogadása csak a mindenki számára hozzáférhető munkaállomásokon történhet. A saját munkagéppel rendelkező munkatársak a saját munkájukkal összefüggő adatokról készíthetnek másolatot.
- Az intézmény részére biztonsági illetve archív adatállomány előállítását az intézményi informatikai felügyeletet ellátó személy végzi kétheti rendszerességgel. A biztonsági másolatok csak az intézményvezető engedélyével adhatók ki.

- A saját tulajdonú adathordozókat használatba venni csak az előírt ellenőrző eljárások (pl. vírusellenőrzés) után szabad.
- Minden adathordozót újra alkalmazás előtt, felszabadítás, selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell.
- A számítástechnikai adathordozók állapotát, elöregedését évente egyszer ellenőrizni kell.

12.2. Az adathordozók nyilvántartása és megőrzése

- A személyes adatokat vagy pályázati anyagokat tartalmazó számítástechnikai adathordozókról nyilvántartást kell vezetni *(Lásd. 1. sz. melléklet)*
- Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni.
- A nyilvántartás az azonosító adaton kívül a felírás és megőrzés dátumát, a betekintésre jogosultakra vonatkozó adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat tartalmazza. A megőrzésre, betekintésre és kiadásra vonatkozó adatokat az adatkezelő határozza meg.
- A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.
- Az adathordozók megőrzési idejét az adatkezelő határozza meg.

12.3. Az adathordozók selejtezése

A fizikailag károsodott, javíthatatlan, a gyári, raktározási hiba következtében felhasználásra alkalmatlan adathordozókat selejtezni kell. A selejtezést selejtezési bizottság végzi és jegyzőkönyvet készít tevékenységéről.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. A bizalmas adatokat tartalmazó adathordozókról törlő programokkal kell az adatokat eltávolítani, majd ezt követően kell fizikailag megsemmisíteni az adathordozót.

13. Az elektronikus nyilvántartások

- Az intézmény alkalmazottai számos országosan vagy kerületi szinten kötelező elektronikus nyilvántartást vezetnek. A hozzáférési jogosultságokat az intézményvezető határozza meg és titkosítva továbbítja a feladatot ellátó személynek. A kötelezően vezetendő elektronikus nyilvántartások hozzáférési jogosultságairól az intézményvezető nyilvántartást vezet. Az információs rendszerek hozzáférési kulcsainak őrzése az intézmény páncélszekrényében zárt borítékban történik.
- Az adatbevitel során bevitt adatok helyességéért a feladat ellátásával megbízott személy felelős és az alkalmazási követelményeknek megfelelően rendszeresen ellenőrzi azokat.
- Az alkalmazottak saját munkájuk megkönnyítése érdekében elektronikus nyilvántartásokat készíthetnek és vezethetnek. Ezen esetekben az adatkezelés, feldolgozás és továbbítás mindig a hatályos jogszabályok előírásainak figyelembevételével, az adatbiztonság megőrzése mellett kell, hogy történjen.

- Külső személy – pl. karbantartás, javítás, fejlesztés céljából – a számítástechnikai eszközökhöz úgy férhet hozzá, hogy a kezelt adatokat ne ismerhesse meg.
- Programfejlesztés vagy próba céljára valódi adatok felhasználását – különösen akkor, ha a próbát külső szerv vagy személy végzi, illetve annak eredményeit megismerheti – el kell kerülni. Ha ez nem valósítható meg, akkor az adatok biztonságát más módszerekkel kell megőrizni.

14. Elektronikus szolgáltatások

14.1. Az adatszolgáltatás általános szabályai

- Minden intézményi felhasználó számára, a neki megfelelő jogosultsági szint alapján, minden adatot biztosítani kell.
- A közérdekű adatokat, valamint a közérdekből nyilvános adatokat, jogosultsági szinttől függetlenül, minden felhasználó számára biztosítani kell.
- Az információkért minden esetben az információ közreadója felelős.
- Minden szolgáltatott információt azonosítani kell a közreadó nevével, az érvénybe lépés időpontjával, a lejárat idejével, dátummal, verziószámmal vagy bármely más módon, amelyből megállapítható a közölt információ érvényessége, hitelessége.
- Az információszolgáltatás megszervezéséért, időben történő továbbításért az információ közreadója a felelős.
- A közreadott információk formátumát és annak továbbítási módját a szolgáltatás üzemeltetője a közreadóval egyeztetve határozza meg és gondoskodik az ehhez szükséges módszerek és szoftverek használatának betanításáról.
- Az összes intézményi információ az intézmény vagyonának részét képezi, ennek megőrzéséről, megóvásáról a rendszergazda, az intézményi informatikai felügyeletet ellátó személy illetve az egyetértésével az információ közreadója köteles gondoskodni.
- A közölt információk az adatvédelmi és szerzői jogi törvényeket, szabályokat nem sérthetik.

14.2. Az elektronikus levelezés

Valamennyi intézményi munkavállaló jogosult az Tankerület által biztosított elektronikus levelezés használatára. Az elektronikus levelezést kezelő szervernek megfelelő DNS bejegyzéssel kell rendelkezniük. Ezt a Tankerület biztosítja. Valamennyi, az iskolában üzemelő e-mail fióknak egyértelműen intézményi felhasználóhoz, vagy szervezeti egységhez kötöttnek kell lennie. Az e-mail fiókért a felhasználó tartozik teljes körű felelősséggel.
Amennyiben az elektronikus levelezési cím egyértelműen azonosítható intézményi felhasználóhoz kapcsolható és részben vagy egészben tartalmazza a felhasználó nevét, úgy a felhasználó levelezése azonos elbírálás alá esik, mint a hagyományos postai levelezés, tehát a levéltitok szabályai ebben az esetben is érvényesek.

Valamennyi, az elektronikus levelezést használó intézményi felhasználó a következő szabályokat köteles betartani a kiküldött leveleivel kapcsolatban:

- a levél nem tartalmazhat a hatályos magyar jogszabályokba ütköző tartalmat;
- a levelezés nem veszélyeztetheti az informatikai infrastruktúra működését;
- tilos a levelek fejlécének hamisítása, félrevezető kitöltése;

- tilos levélbombák, levelezési láncok küldése, továbbítása;
- tilos kéretlen vagy vírusos levelek küldése, továbbítása.

14.3. Az intézmény honlapja

Az intézmény központi honlapjának címe: www.prizmaegymi.hu. A honlapot az intézményi informatikai felügyeletet ellátó személy üzemelteti:

- biztosítja a honlap publikus szolgáltatásként való működését (figyelemmel kíséri a személyi, szervezeti változásokat, egyéb döntéseket, határozatokat és ennek megfelelően módosítja a központi honlap tartalmát),
- rendszeresen biztonsági mentést készít róla;
- felügyeli a honlap szerkezeti integritását;
- a honlap fejlesztésével, új tulajdonságokkal, funkciókkal való kibővítésével kapcsolatban összegyűjti az igényeket és a fejlesztőknek továbbítja.
- kiadja a honlap szerkesztéséhez szükséges azonosítókat, jelszavakat. Ezek titokban tartásáért minden felhasználó teljes körű felelősséggel tartozik.
- A honlapra bármilyen tartalmú dokumentumot, fényképet, stb. csak az intézményvezető, vagy tagintézményvezető jóváhagyásával lehet.

15. Záró rendelkezések

Az Informatikai Biztonsági Szabályzat megismerését az intézmény dolgozói részére évente egyszer, az informatikai felügyeletet ellátó személy, oktatás formájában biztosítja.

Az intézményi Informatikai Biztonsági Szabályzatban foglaltakról az alkalmazotti testület tagjai véleményt nyilvánítanak.

Az intézményi Informatikai Biztonsági Szabályzatot az alkalmazotti testület 2017. október –i ülésén véleményezte és …… /2010. számú határozatával elfogadta.

Budapest, 2017.

.....
intézményvezető

16. A szabályzat mellékletei

1. sz. melléklet - Intézményi adathordozók nyilvántartása
2. sz. melléklet - Elektronikus nyilvántartásokhoz való hozzáférési jogosultságok nyilvántartása

INTÉZMÉNYI ADATHORDOZÓK NYILVÁNTARTÁSA

Azonosító szám	Rövid megnevezése	Felírás dátuma	Megőrzési határidő	Betekintésre jogosultak	Adathordozó kiadhatósága	Kiadva	Visszavéve

ELEKTRONIKUS NYILVÁNTARTÁSOKHOZ VALÓ HOZZÁFÉRÉSI JOGOSULTSÁGOK NYILVÁNTARTÁSA

Elektronikus nyilvántartás megnevezése	Hozzáférésre, adatkezelésre jogosult személy neve	Hozzáférési jogosultság kiadása	Hozzáférési jogosultság visszavétele