Ebesi Arany János Magyar–Angol Két Tanítási Nyelvű
Általános Iskola és Alapfokú Művészeti Iskola
4211 Ebes, Széchenyi tér 5.
Tel: (52) 565-023 Fax: (52) 565-022
E-mail: iskolatitkar@arany-ebes.sulinet.hu
www.ebesarany.hu

OM azonosító: 031172 Szervezeti egységkód: HB3601

Informatikai és Biztonsági Szabályzat

az

EBESI ARANY JÁNOS MAGYAR - ANGOL KÉT TANÍTÁSI NYELVŰ
ÁLTALÁNOS ISKOLA ÉS ALAPFOKÚ MŰVÉSZETI ISKOLA

részére

2019.

Tartalom

Az Informatikai és Biztonsági Szabályzat törvényi háttere

2001. évi CXXI. törvény

A törvény a Büntető Törvénykönyv 2002. április 1-től hatályos módosítását tartalmazza. A Büntető Törvénykönyvbe új vétségek és bűncselekmények kerültek be, mégpedig a következők:

• „*Számítástechnikai rendszer és adatok elleni bűncselekmény*" és

• „*Számítástechnikai rendszer védelmet biztosító technikai intézkedések kijátszása*".

A fenti kategóriák a Btk. 300/C illetve 300/E paragrafusában találhatók.

A 300/C passzus szerint a törvény bünteti, ha valaki „*számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad*". Ezen kívül büntetendő az is, aki „*számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz*" illetve „*adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza*". A büntetés lehet szabadságvesztés, pénzbüntetés vagy közérdekű munka. Ugyanennek súlyosbított változata, ha mindezt jogtalan haszonszerzés miatt követi el valaki.

A 300/E paragrafus szerint büntetendő, aki „*a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot*

a) készít,

b) megszerez,

c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz",

illetve ha ilyen ismeretet más rendelkezésére bocsátja. A büntetés alól felmentést jelent, ha valaki tevékenységét a hatóságok előtt felfedi. A törvény a fenti esetekre igen szigorú büntetéseket szab ki, egyes esetekben a büntetés mértéke megegyezik az emberölés alapesetének büntetésével.

A 300/F paragrafus :

„*A 300/C. § és a 300/E. § alkalmazásában számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége.*"

2011. évi CXII.törvény

25/I. § (1) „Az adatkezelő és az adatfeldolgozó a kezelt személyes adatok megfelelő szintű biztonságának biztosítása érdekében az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető - így különösen az érintettek különleges adatainak kezelésével járó - kockázatok mértékéhez igazodó műszaki és szervezési intézkedéseket tesz."

137/2016. (VI. 13.) Korm. rendelet

A Kormány az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 105. § (1) bekezdés g) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva rendeli el a elektronikus aláírásra vonatkozó szabályokat.

1. Hálózathasználati szabályzat

1.1 Bevezetés

Az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola hálózata jelenleg egy publikus hálózathoz kapcsolódik:

- Sulinet – Közháló

A szabályzat az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola Informatikai Biztonsági Szabályzatának többi rendelkezésével együttesen alkalmazandó, a szabályzat által nem tárgyalt kérdésekben Magyarország hatályos törvényei az irányadók.

1.2 A szabályzat hatálya

Jelen utasítás mindenkire nézve kötelező, aki használja az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola számítógép hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola számítógép-hálózatát használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

1.3 A hálózat használatának szabályai

Az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola hálózata nem használható az alábbi tevékenységekre :

- a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
- profitszerzést célzó, 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 igénybevevő tevékenység (pl. levélbombák, hálózati játékok, kéretlen reklámok);
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása (pl. TCP port scan);
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására,

megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;

- másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok közzététele);
- hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

1.4 Felelősök

Felelősöket kell kinevezni, akik ellenőrizzék a hálózat egyes részeinek, szolgáltatásainak működését, rendeltetésszerű és szabályos használatát, valamint felelnek a biztonsági előírások betartásáért és betartatásáért. A felelősöket az intézményvezető jelöli ki, róluk elérhetőségükkel együtt nyilvántartást kell vezetni, ezeket a listákat naprakészen tartani, és rendszeres időközönként (legalább félévente) ellenőrizni.

Az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola vezetője ezen feladatok ellenőrzésével, felelősként a Csiha László rendszergazdát bízza meg.

1.5 A felhasználók kötelességei

A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében.

A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

1.6 A felhasználók jogai

- Minden iskolai diáknak joga van tanítási órákon hozzáférni az intézmény informatikai szolgáltatásaihoz.
- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetői tiszteletben tartják, ettől eltérni csak a törvény által meghatározott esetekben lehet.
- A rendszer technikai problémáiról (tervezett vagy rendkívüli eseményekről) tájékoztatni kell a felhasználókat.
- A felhasználók számára elérhető módon közzé kell tenni a felhasználókra vonatkozó szabályok érvényes változatát.

1.7 Szankciók

A Szabályzat megsértésének gyanúja esetén az esetet ki kell vizsgálni, és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket, amelyre a következők az irányadók:

- A Szabályzat előírásainak nem ismerete nem mentesít a következmények vállalásának kötelességétől.
- A Szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.

- A Szabályzatnak egy figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül.
- A Szabályzat szándékos megsértése esetén az elkövető a hálózat használatából ideiglenesen vagy véglegesen kizárható, és az eset súlyosságától függően fegyelmi eljárás folytatható le ellene.
- A szándékos elkövető köteles megtéríteni az általa okozott károkat a Polgári Törvénykönyv előírásai szerint.
- Ha az elkövetett cselekedet kimeríti valamely hatályos magyar törvény tényállását, akkor a felelősnek kötelessége megtenni a megfelelő törvényi lépéseket.

2. Jelszókezelési szabályzat

2.1 Bevezetés

A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mert egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a jelszó tulajdonosára, hanem az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola informatikai rendszerére is negatív következményekkel járhat. A jelszavaknak két nagy csoportját különböztethetjük meg a következők alapján: adminisztrátori vagy egyszerű felhasználói jogú azonosítót véd a jelszó, a szabályozás ennek függvényében eltérhet, az adminisztrátori jelszavakra mindig a szigorúbb szabályok érvényesek.

2.2 A szabályzat hatálya

Jelen szabályzat mindenkire érvényes, aki az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola hálózatának bármely részéhez jelszó használatát igénylő hozzáféréssel rendelkezik.

2.3 Alapelvek

- Nem szabad könnyen kitalálható jelszavakat választani! (A helyes jelszóválasztáshoz a 2.4-es fejezet ad segítséget.)
- A jelszavakat mindenképp titokban kell tartani! (A jelszavak védelméről a 2.5-ös fejezetben található útmutató.)
- Az induló jelszót az első bejelentkezéskor meg kell változtatni.
- A jelszavakat rendszeres időközönként cserélni kell (adminisztrátori jelszó esetén 3 havonta ajánlott, egyéb esetben félévente).
- Új jelszónak nem szabad az utolsó 5 régi közül egyiket sem megadni.
- Ha a felhasználónak gyanúja támad, hogy jelszava kompromittálódhatott, azonnal meg kell változtatnia.
- 5 sikertelen próbálkozás után a felhasználói fiók zárolandó.
- A jelszavakat nem szabad kódolatlanul tárolni.
- Azon személyek, akik különböző rendszerekhez, illetve több felhasználói azonosítóval is rendelkeznek, a különböző rendszerekhez, azonosítókhoz különböző jelszavakat kell használniuk.
- Ahol lehetséges, a jelszavakra vonatkozó alapszabályokat (jelszóhossz, jelszócsere, előző jelszavak megadásának tilalma) az adott informatikai rendszer segítségével ki kell kényszeríteni.

2.4 Helyes jelszóválasztás

- Nem szabad könnyen kitalálható, személyre jellemző jelszavakat használni (pl. személyes adatok, családtagok, barátok neve, házi kedvenc neve…).
- A jelszónak legalább 7 karakter hosszúnak kell lennie.
- Nem szabad sorozatokat használni (pl. abcdefg, 7654321, asdfghj).
- Kerülni kell a szótári szavak használatát (ezek egy számjeggyel kiegészített változatai sem biztonságosak).
- A jelszó tartalmazzon kis- és nagybetűket, lehetőleg számokat és speciális karaktereket is.
- A nemzeti billentyűzet állíthatósága miatt nem javasolt az ékezetes karakterek, az Y, a Z és a 0 (nulla) használata.
- A jelszónak könnyen megjegyezhetőnek kell lennie. Könnyen megjegyezhető erős jelszavak például a jelmondat alapú betűszavak. Választunk egy kedvenc mondatot (szólást vagy idézetet akár), pl.: „**K**i **i**tt **b**elépsz, **h**agyj **f**el **m**inden **r**eménnyel!”, majd ennek kezdőbetűiből összeállítunk egy betűszót: „kibhfmr”. Ezt utána variálhatjuk nagybetűkkel, számokkal, jelekkel, pl.: „kiB3hfmR-”, és kész az erős jelszó, amit később mégse lesz nehéz felidézni.
- Végül pedig: Ne használjuk a példákban felsorolt jelszavakat!

2.5 Jelszóvédelem

A jelszót titokban kell tartani, másokkal azt nem szabad megosztani (családtagokkal, barátokkal sem). A legerősebb jelszó sem ér semmit, ha azt könnyen elérhető helyen tartjuk, vagy könnyen megszerezhető. Különösképpen figyelni kell az alábbiakra:

- A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
- A jelszót se a feljebbvalóknak, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, ha kifejezetten kérik ezt, akkor sem.
- Tilos közös jelszavakat használni (még családtagokkal, barátokkal sem szabad).
- A jelszót nem szabad leírni, és elérhető helyen tárolni (irodában, táskában…).
- A jelszót nem szabad semmilyen számítógépes rendszeren titkosítás nélkül (pl. egyszerű szövegfájlban) tárolni.
- A jelszót nem szabad telefonon vagy e-mail-ben továbbítani.
- Ne utaljunk a jelszó tartalmára (pl. „a kedvenc együttesem neve”).
- Ne használjuk a programok jelszó megjegyző funkcióját.
- A jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott, vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni a jelszót, és értesíteni kell a rendszergazdát.
- Cseréljük jelszavunkat legalább félévente (adminisztrátori jelszavaknál az ajánlott periódus 3 hónap). A jelszavak véletlen támadásoknak is áldozatul eshetnek, ezért fontos a rendszeres jelszócsere.

3. Vírusvédelmi szabályzat

3.1 Bevezetés

A számítógépes vírusok a számítógépen tárolt adatok és programok kártevői. A vírus a megfertőzött program futása közben másolja, többszörözi önmagát. Rendszerbe kerülésük történhet fertőzött lemeztől történő rendszerindítási kísérlet (bootvírusok), egy fertőzött program elindítása (fájlvírusok), egy vírusos makrókat tartalmazó dokumentum megnyitása (makrovírusok), Internet használat közben (etikailag nem javasolt tartalmak látogatása) vagy e-mail-ben csatolt állományként terjedő makró- illetve script vírusok, férgek megnyitásának eredményeként. A vírusok gépről gépre terjednek, többnyire észrevehetetlenek, amíg nem aktivizálódnak. Ekkor azonban nagy kárt okozhatnak pótolhatatlan adatok megsemmisítésével, a rendszer bénításával, bizonyos esetekben hardveres károkozással. A víruskeresők, vírusirtók használata elengedhetetlen, de ezek is csak a már ismert vírusok ellen jelentenek igazi védelmet.

Ez a szabályzat az előbbiekben felsorolt káros hatások megelőzésére, és a vírusfertőzés esetén elvégzendő teendők leírására szolgál.

3.2 A szabályzat hatálya

A vírusvédelmi szabályzat minden az iskola hálózatába kötött személyi számítógépre, pda-ra és szerverre/szerverekre vonatkozik.

3.3 Vírusfertőzés gyanús helyzetek

Sok jele lehet vírus jelenlétének, azonban ezek nagy része normál tevékenység eredményeként is előállhat. Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt – vírusfertőzésre utaló – jelenségekkel:

- A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.
- Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő. Nagyon erős vírusjegy.
- Szokatlan és váratlan képernyő tevékenység (szokatlan üzenetek, ablakok megjelenése). Erős vírusjegy.
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak). Általánosan erős vírusjegy. Ha az operációs rendszer újraindítása után is fennáll, erős vírusjegynek tekinthető.
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy. Helytelen rendszerkonfiguráció is okozhatja.

3.4 Vírusvédelmi teendők

Az alábbi utasítások betartása erősen ajánlott a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében:

- Vírusvédelmi szoftvert kell használni. Biztosítani kell a szerverek, a munkaállomások vírusvédelmét. Jelenleg az intézmény a Microsoft Security Essential vírusvédelmi programot használja minden munkaállomásán.
- A vírusvédelmi programnak rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik, és állandó háttérvédelmet biztosít. A felhasználóknak nem szabad kikapcsolni ezt a védelmet.
- Ne fusson egyszerre két vírusölő program.
- Kéthetente minden gépen teljes vírusellenőrzést kell végrehajtani (a vírusvédelmi szoftver támogatja az időzített keresési funkciót).
- A vírusvédelmi program vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell. Ha erre lehetőség van, az automatikus frissítést kell választani, így az új elemek rögtön megjelenésük után felkerülhetnek a rendszerre.
- Idegen helyről származó adattárolókon (floppy, cd, dvd, pen-drive, HDD) használat előtt vírusellenőrzést kell végezni.
- Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.
- Az Office csomagok programjainál, ahol lehet, be kell állítani a makrók jelenlétének kijelzése funkciót. Idegen állományokat csak makrók futtatása nélkül opcióval szabad megnyitni.
- Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mail-ek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket. Az e-mailben küldött vírusok, férgek rendszeresen operálnak valamilyen különös megjegyzéssel a levelek tárgy bejegyzésében.
- A fontos adatokról és a rendszerkonfigurációról készüljön archiválás.

3.5 Teendők vírusfertőzés esetén

- Tájékoztatni kell a vírusvédelemért felelős személyt (számítástechnika tanárt, operátort, rendszergazdát) a fertőzésről vagy annak gyanújáról.
- A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).
- A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.
- A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál.
- Ezek után a rendszer újraindítható a szokott módon.

4. Távoli elérés szabályzata

4.1 Bevezetés

A szabályzat célja, hogy irányt mutasson az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola belső hálózatához távoli gépről történő csatlakozáshoz. A szabályzat betartásával megakadályozható, hogy az iskola hálózatát, informatikai rendszerét a nem jogosult felhasználásból eredő károk érjék. A károk magukban foglalják az érzékeny adatok elvesztését, az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola hírnevének károsodását, illetve az iskola belső rendszerének sérülését.

4.2 A szabályzat hatálya

Az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola hálózatának távoli elérésére a iskolai szerver/szerverek távoli elérésének keretében van lehetőség: intranet kapcsolat, fájlcsere szolgáltatás, távoli asztal. A szabályzat mindhárom típusú kapcsolatra vonatkozik, valamint kiegészül a szolgáltatások igénybevételénél elfogadott rendelkezésekkel.

4.3 Szabályok

- A bejelentkezés időtartamára a felhasználóra érvényes az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola Hálózathasználati Szabályzata.
- A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító / jelszó megadása).
- A belépési azonosítókat másra átruházni, illetve más azonosítóját használni nem szabad.
- A belépési adatokat senkinek sem szabad elárulni.
- A bejelentkezéseket ellenőrizni és naplózni kell.
- Távoli bejelentkezés adminisztrátori jogokkal csak biztonságos, birtokláson és jelszón alapuló felhasználói azonosítással lehetséges.
- A távoli elérésnek biztonságos kapcsolaton keresztül kell megvalósulnia (telnet helyet SSH, FTP helyett SFTP vagy SCP, vagy valamilyen biztonsági protokollon keresztül).
- A bejelentkezett végpontot nem szabad felügyelet nélkül hagyni, még rövid időre sem.
- 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani.
- Behívó szerveres kapcsolat esetén, ha a végpont az Internetre másik csatornán keresztül is csatlakozik, tűzfal használata kötelező.

5. Szerver biztonsági szabályzat

5.1 Bevezetés

A szabályzat célja, hogy az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola szervereire olyan követelményeket és alapbeállításokat határozzon meg, amik a biztonságos használatot elősegítik. Jelen szabályzat alapelveket határoz meg, mivel konkrét utasítások megfogalmazása a különböző szerverek különböző operációs rendszerei és szolgáltatásai miatt nehézségekbe ütközne.

5.2 A szabályzat hatálya

A szabályzat vonatkozik minden az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola tulajdonában, illetve felügyelete alatt levő szerverre, valamint az ebesarany.hu tartomány alatt található összes szerverre.

5.3 Alapelvek

- Az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola hálózatába kapcsolt szervereket az intézményvezetőnél be kell jelenteni, ezekről a titkárság nyilvántartást vezet. Bejegyzetlen szerver nem működhet a iskola hálózatán.
- A szerverekről minimálisan a következő információkat nyilván kell tartani:
  - A szerver fizikai helye
  - A felelőse (elérhetőségével együtt)
  - Hardver konfigurációja és operációs rendszere
  - Főbb funkciói és szolgáltatásai

  Ezeket az információkat naprakészen kell tartani.
- A szervereket a rendszergazdai szobában kell elhelyezni. A szerverekhez való hozzáférést fizikailag is korlátozni kell.
- A szervereknek illetéktelen behatolástól jól védettnek kell lennie (megfelelő alapbeállítások használata, majd upgrade-k, biztonsági javítások mielőbbi telepítése).
- A szerverek konzoljairól az adminisztrációs tevékenység befejeztével ki kell lépni, nem szabad felügyelet nélkül bejelentkezve hagyni.
- Hacsak nem szükséges feltétlenül, nem szabad adminisztrátori jogosultságokkal használni a szervert.
- A szervereken le kell tiltani minden nem használt szolgáltatást.
- Ha adottak a technikai lehetőségek, a biztonságos kapcsolatfelvételt kell preferálni, adott esetben csak az ilyen típusú hozzáférést szabad engedélyezni (telnet helyett SSH, FTP helyett SFTP, SCP használata).

- A szerverhez illetve szolgáltatásaihoz történő hozzáférési kísérleteket naplózni kell, és ezeket a naplókat rendszeresen ellenőrizni kell.
- A biztonsági mentéseket minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.
- A biztonsági eseménynaplók, mentések esetében az őrzési idő a mindenkori hatályos jogszabályokban foglaltaknak megfelelően kell eljárni.

6. Felhasználó kezelési szabályzat

6.1 Bevezetés

Az informatikai rendszer használatával való visszaélés kizárása érdekében minden felhasználónak egyedi felhasználó azonosítóval és az ahhoz tartozó jelszóval kell azonosítania magát. Felhasználó az iskola dolgozója vagy tanulója lehet, egyéni elbírálás alapján külső személy is kaphat felhasználó azonosítót.

Mivel sok és sokféle rendszerre lehet felhasználó azonosítót létrehozni, ezért az alábbiakban csak általános vezérelvek lesznek felsorolva.

6.2 A szabályzat hatálya

A szabályzat érvényre juttatási körébe tartoznak mind az operációs rendszerhez, mind egyes alkalmazásokhoz hozzáférési jogot biztosító felhasználói azonosítók az iskolai hálózat bármely részére vonatkozólag.

6.3 Alapelvek

- A felhasználó azonosítók kiadása központilag történik minden rendszer esetében.
- Felhasználó azonosítót írásban kell igényelni.
- Azonosító igénylésekor egyértelműen meg kell határozni a jogosultságot birtokló, azért felelősséggel tartozó személyt. Ellenőrizni kell, hogy az igénylő jogosult-e a felhasználó azonosítóra (tanulók esetében érvényes diákigazolvány, dolgozók esetében a munkáltatói jogú felettes igazolása).
- A felhasználónak aláírásával kell igazolnia, hogy a használat feltételeit és szabályait megismerte, és azokat magára nézve kötelezőnek tekinti.
- Adminisztrátori feladatokat ellátó személyek részére a normál felhasználói feladatok ellátására és adminisztrációs célokra külön azonosítót kell létrehozni.
- A különböző hozzáférési jogosultságok a felhasználó azonosítóhoz kapcsolódnak.
- Az azonosításnak (és ha szükséges hitelesítés) meg kell előznie az informatikai rendszernek a felhasználóval kapcsolatos valamennyi más kölcsönhatását.
- A felhasználó azonosítót le kell tiltani, ha azzal visszaélés történt, és az esetet ki kell vizsgálni.
- A felhasználó azonosítókat a rendszerből törölni kell, ha a felhasználó már nem a iskola diákja vagy munkavállalója, illetve már nincs az adott rendszer használatához joga.

6.4 A felhasználók kötelességei

Az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola minden munkavállalója és diákja anyagi felelősséggel tartozik, a számára munkavégzés, oktatás céljából biztosított számítástechnikai eszköz után. Ha az intézmény harmadik

félnek is lehetőséget biztosít számítástechnikai eszközeinek használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

7. Mentési és archiválási szabályzat

7.1 Bevezetés

Az elektronikusan tárolt adatok folyamatosan ki vannak téve a hardver meghibásodásának lehetőségének, ezért a biztonság növelése és a károk csökkentése érdekében szükség van rendszeres mentésekre. Míg a mentések fő feladata a biztonsághoz kapcsolódik, addig az archiválás egy korábbi állapot tárolását szolgálja. Ez utóbbinak biztonsági incidensek bekövetkezése esetén lehet fontos szerepe, a napló és log fájlokban, valamint egyéb adatok között értékes információkat, nyomokat lehet találni a biztonsági esemény bekövetkezésével kapcsolatban. Technikai megvalósításuk hasonlósága miatt kerülnek egy helyen tárgyalásra.

7.2 A szabályzat hatálya

A szabályzat érvényes minden az Ebesi Arany János Magyar - Angol Két Tanítási Nyelvű Általános Iskola és Alapfokú Művészeti Iskola tulajdonában, illetve felügyelete alatt levő szerverre, személyi számítógépre.

7.3 Feladatok

- Ki kell jelölni azokat a személyeket, akiknek a biztonsági mentéseket illetve archiválásokat el kell végezniük. Ezt dokumentálni is kell.
- Hetente teljes biztonsági mentést kell végezni a rendszerről, a köztes időben pedig naponta inkrementális mentés készítése szükséges. Az ehhez szükséges adathordozókat rotálni lehet.
- Havonta, évente teljes rendszerarchiválást kell készíteni, és ezeket megőrizni. Ehhez biztosítani kell a megfelelő számú adathordozó egységet.
- A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák.
- On-line rendszerek esetén hideg mentést kell alkalmazni.
- A biztonsági mentéseket és archiválásokat tartalmazó adathordozókat minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.
- A mentéseket tartalmazó adathordozókon jól láthatóan fel kell tüntetni a mentett rendszer nevét, a mentés típusát és idejét.
- A biztonsági eseménynaplókat 1 évre visszamenőleg, a teljes mentéseket pedig a törvényben foglalt ideig meg kell őrizni.
- Legalább évente visszatöltési kísérletet kell végezni a technika megfelelőségének ellenőrzése érdekében.

A Szabályzat az aláírás után hatályba lép.

Ebes, 2019. május 24.

_____

intézményvezető