Informatikai és Biztonsági Szabályzat

2015/2016

P.H.

.....
esperes-főigazgató

.....
igazgató

Informatikai és Biztonsági Szabályzat

a

Tiszakécskei Református Általános Iskola és Gimnázium

részére

Előszó

Mai világunkban egyre fontosabb szerepe van a számítógépeknek az azokat hálózatba kötő telekommunikációs rendszereknek. Az élet különböző területein ma már elképzelhetetlen a számítógép és az Internet használata nélkül boldogulni. Az állami, az oktatási és a gazdasági szféra munkavégzése egyaránt a számítógépek használatán alapul, így a számítógépes rendszerektől való függés egyre nagyobb és nagyobb lesz. A termelés, irányítás, oktatás által keletkezett információk, adatok nagy része már nemcsak papír alapon, hanem nagyrészt informatikai rendszerekben tárolódik. A világhálózat, az Internet terjedésével a kommunikáció és a világban való tájékozódás módja is megváltozik. Ebben az új világban az információ valódi értékké vált és annak védelme immáron elengedhetetlen. De nemcsak az adatot, információt, hanem magát a számítógépes rendszert is védeni szükséges, hiszen ezek támogatása nélkül könnyen megbénulhat a számítógépek által át meg átszőtt életünk.

Az informatikai biztonság, mint kedvező állapot elérése érdekében védelmi intézkedéseket kell alkalmaznunk. Ezeknek az intézkedéseknek át kell fogniuk az informatikai rendszer teljes életciklusát (létesítés, használat, változtatás, megszüntetés), és a védelemre fordított összeg arányban kell, hogy álljon az információ vagy a rendszer sérüléséből okozható kárral. Az informatikai rendszer védelme ki kell hogy terjedjen a fizikai, a logikai, a humánpolitikai védelem területére, valamint speciális eszközök és eljárások használatára.

Ezt a védelmet nehezíti, hogy a számítógépes rendszerek bonyolultsági foka egyre nő. Manapság a legjobb szakemberek is nehéz helyzetben vannak, hiszen ebből a bonyolultságból adódóan nem ismerhetik részleteibe menően a pontos működési mechanizmusokat, így rendkívül nehéz arról meggyőződniük, hogy egy rendszer tényleg úgy működik-e, ahogy kellene, valóban biztonságos-e vagy sem. Egy átlagos felhasználó (egy irodai dolgozó, akinek kezében a számítástechnikai rendszer és szoftver nem cél, hanem csak használati eszköz), még ennyire sem ismeri a számítógépet (ugyanúgy ahogy a mikrohullámú sütő vagy televízió működését sem ismeri pontosan, csak használatának módját). Nehezen tudja eldönteni, hogy egy adott rendszert használva mennyire van kiszolgáltatva a számítógépen keresztül rosszindulatú embertársainak. Az előbbi példában ehhez nyújt segítséget a használati utasítás, amiből megtudhatja mindenki, hogy az elvárt funkcionalitás érdekében mit kell tennie, valamint a saját és környezete biztosságát hogyan tudja megóvni. Ilyen használati utasítás a számítástechnikai rendszerekhez az Informatikai Biztonsági Szabályzat, mely segít a helyes és biztonságos használat elsajátításában.

Ezen felül a rendszer folyamatos működésére nézve az egyes természeti tényezők (tűz, víz, villámcsapás, ...) és a hardver meghibásodások is komoly veszélyt jelentenek, az adatok megsemmisülése mindennapos veszély. Ez a bizonytalanság bizalmatlanságot okoz, és a számítógépes rendszerek terjedését tekintve jelentős negatív hatása van.

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.*"

1992. évi LXIII. törvény

„*10. § (1) 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 e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.*

(2) Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen."

A törvényt a 2003. évi XLVIII. törvény módosította európai uniós jogharmonizációs kötelességek miatt.

2001. évi XXXV. törvény

A 2001-ben elfogadott, majd 2004-ben módosított törvény az elektronikus aláírás jogi szabályozásának alapjait teremti meg.

2001. évi CVIII. törvény

A törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szól, a 2003. évi XCVII. törvény módosította rendelkezéseit. A törvény összhangban van az Európai Unió 2000/13/EC jelű, azonos témájú irányelvével.

Szabályzat

1. Hálózathasználati szabályzat

1.1 Bevezetés

A Tiszakécskei Református Általános Iskola és Gimnázium hálózata jelenleg két publikus hálózathoz kapcsolódik:

- Sulinet – Közháló
- T-Online Internet

A szabályzat a Tiszakécskei Református Általános Iskola és Gimnázium Informatikai Biztonsági Szabályzatának többi rendelkezésével együttesen alkalmazandó, a szabályzat által nem tárgyalt kérdésekben a Magyarország hatályos törvényei az irányadók.

1.2 A szabályzat hatálya

Jelen utasítás mindenkire nézve kötelező, aki használja az Tiszakécskei Református Általános Iskola és Gimnázium számítógép hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed a Tiszakécskei Református Általános Iskola és Gimnázium összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz a Tiszakécskei Református Általános Iskola és Gimnázium 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

A Tiszakécskei Református Általános Iskola és Gimnázium 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 kontrollálják a hálózat egyes részeinek, szolgáltatásainak működését, rendeltetésszerű és szabályos használatát, valamint felelnek a biztonsági előírások betartásáért és betartatásáért. A felelősöket az igazgató jelöli ki, róluk elérhetőségükkel együtt nyilvántartást kell vezetni, ezeket a listákat naprakészen tartani, és rendszeres időközönként (legalább félévente) ellenőrizni.

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

- 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 a Tiszakécskei Református Általános Iskola és Gimnázium 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 a Tiszakécskei Református Általános Iskola és Gimnázium 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 a gimnázium hálózatába kötött személyi számítógépre, pdara 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 és a pdak vírusvédelmét. 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.
- A MS-Office csomag 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 (informatika 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. Szerver biztonsági szabályzat

4.1 Bevezetés

A szabályzat célja, hogy a Tiszakécskei Református Általános Iskola és Gimnázium 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.

4.2 A szabályzat hatálya

A szabályzat vonatkozik minden a Tiszakécskei Református Általános Iskola és Gimnázium tulajdonában található összes szerverre.

4.3 Alapelvek

- A Tiszakécskei Református Általános Iskola és Gimnázium hálózatába kapcsolt szervereket az igazgatónál be kell jelenteni, ezekről a titkárság nyilvántartást vezet. Bejegyzetlen szerver nem működhet a gimnázium 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.

5. Felhasználó kezelési szabályzat

5.1 Bevezetés

Az informatikai rendszer használatával való visszaélés kizárása érdekében minden felhasználónak egyedi felhasználó azonosítóval és az ahhoz tartozó jelszóval kell azonosítania magát. Felhasználó a gimnázium 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.

5.2 A szabályzat hatálya

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

5.3 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 gimnázium diákja vagy munkavállalója, illetve már nincs az adott rendszer használatához joga.

5.4 SuliX rendszer

A Tiszakécskei Református Általános Iskola és Gimnázium 2013 szeptemberétől csatlakozott a SuliX operációs rendszert felhasználók közé. A rendszerben kialakításra került minden tanárnak és diáknak egyedi felhasználónév. A felhasználónévhez jogosultsági körök tartoznak. A diákok az iskola egész területén tanítási idő alatt és kívül nem használhatják a közösségi portálókat (facebook, iwiw, stb) illetve a videó megosztó portálokat (youtube, indavideo, stb.). A pedagógusokra nem vonatkozik semmilyen korlátozás, Az informatikai rendszer kialakítása ennek megfelelően történt. Az elektronikus napló használatának megkönnyítése érdekében az iskola egész területén elérhető vezeték nélküli internetes hálózat, melyet kizárólag tanári jelszóval lehet elérni.

5.5 A felhasználók kötelességei

A Tiszakécskei Református Általános Iskola és Gimnázium 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.

Tiszakécske, 2015. szeptember 1.

Balla Norbert Csaba

.....

Balla Norbert Csaba
rendszergazda