

Apagyi Zrínyi Ilona Általános Iskola
Informatikai biztonsági szabályzat

2024.

Tartalom

Általános rendelkezések,	3
Definíciók	3
A szabályzat hatálya	4
A hálózat használatának szabályai.....	4
Oktatást támogató eszközök	5
A hálózat külső vagy belső szolgáltatásait használó személy felelőssége:.....	5
Adatbiztonság	6
Szerver biztonsági szabályzat	7
Vírusvédelmi szabályzat	7
Az informatika terem használatával kapcsolatos szabályok	9
A tiltott és használatban korlátozott tárgyakra vonatkozó további szabályok	10

Általános rendelkezések,

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, valamint megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzatban meghatározott védelemnek működni kell a rendszerek fennállásának egész időtartama alatt, a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig terjedő életciklusukban.

Az IBSZ 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 jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

Definíciók

Felhasználó fogalmának definiálása

Az intézmény Informatikai rendszerét elérő, azt használó személy.

Intézményi Informatikai rendszer (hálózat):

Az iskola Informatikai rendszere és a hálózatra csatlakozott felhasználók (eszközök), tehát külső vagy belső szolgáltatásokat elérő személyek és az ezt biztosító infrastruktúra összessége.

A hálózatban működő eszközök definiálása, felelőségek, feladatkörök:

Intézményi eszköz - biztonságáért a rendszergazda a felelős, működtetéséért a megbízott személy a felelős;

Saját tulajdonú eszköz - működtetéséért-biztonságáért a tulajdonló személy felelős;

Használatra kiadott eszköz – Működtetéséért-biztonságáért az eszközt kezelő/használó személy a felelős;

A szabályzat hatálya

Jelen utasítás mindenkire nézve kötelező, aki használja az Apagyi Zrínyi Ilona Általános Iskola hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed Apagyi Zrínyi Ilona Általános Iskola összes tanulójára és dolgozójára, aki oktatási vagy az intézmény adminisztrációs feladataihoz az Apagyi Zrínyi Ilona Általános Iskola számítógép-hálózatát használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

A hálózat használatának szabályai

Az oktatást támogató céllal az Apagyi Zrínyi Ilona Általános Iskola az EFOP 3.2.4. keretében országosan létrehozott központilag kezelt eduroam wifi hálózatot, illetve központilag kezelt vendég wifi hálózatot használ az intézmény teljes területén.

Az EFOP324 keretében országosan központilag üzemeltetett eduroam hálózathoz hozzáférést a rendszergazdánál lehetséges igényelni. A létrehozott accounttal bármely (alap/közép/felsőoktatási) intézményben található eduroam hálózathoz csatlakozni lehet. Külföldi oktatási intézményekben található eduroam hálózatokra ugyanez igaz.

Az EFOP 324 keretében felszerelt Wifi hálózat országos központi üzemeltetésű, annak helyes működéséért országosan a KIFÜ által megbízott üzemeltetők a felelősek.

Az Apagyi Zrínyi Ilona Általános Iskola hálózata nem használható az alábbi tevékenységekre:

- a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmozás), tiltott hasznoszerzésre 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 rendeltetészerű 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 érzékenységet 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).

Oktatást támogató eszközök

Saját tulajdonú eszköz esetén a felhasználó köteles eszköze szabályos biztonságos működéséért felelősséget vállalni, hogy más felhasználókat, vagy a hálózat integritását ne veszélyeztesse.

Ez takarja:

- Az eszköz időszaki karbantartását;
- Vírusmentesen tartását;
- szervizelését.

Intézményi (vagy névre kiadott intézményi) eszköz esetén a nem rendszerű használatból eredő kárért a felhasználó a felelős, egyéb meghibásodás vagy probléma esetén a rendszergazdától/megbízott személytől lehet segítséget kérni.

Felhasználó feladata intézményi eszköz esetén: a neki kiadott vagy általa kezelt nem saját eszköz állagának megőrzése rendeltetésszerű használata. Az általa használt internet szolgáltatás rendeltetésszerű használata.

A hálózat külső vagy belső szolgáltatásait használó személy felelőssége:

A rendszergazda feladata az intézményi hálózat / informatikai infrastruktúra karban tartása üzemeltetése, segítségnyújtás a felhasználóknak a hálózat külső / belső szolgáltatásainak elérésében, Informatikai eszközök karbantartása szervizelése, vagy az azzal megbízott szervezettel kapcsolattartás.

A felhasználók jogai:

- Minden iskolai diáknak joga van tanítási órákon hozzáférni az intézmény informatikai szolgáltatásaihoz.

Informatikai biztonsági szabályzat

- 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.

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 köteleességétől.
- 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.

Adatbiztonság

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.

Az intézményben tárolt adatok fizikailag védett zárt (külön e célra kialakított / szeparált) helyen vannak tárolva.

Az adatok több példányban vannak tárolva. A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák.

A helyileg tárolt intézményi adatok mentéséért a rendszergazda a felelős.

Bármely tárolt adat tartalomért az adatkezeléssel megbízott adatkezelő a felelős.

Online adminisztrációs felületek adatbiztonságáért, ezen szolgáltatások üzemeltetői vállalnak felelősséget (pl.: E-napló).

Személyes online adataink elérése esetében az illető szolgáltató vállal felelősséget adatbiztonságunkért.

Bármely Wifi vagy helyi hálózati szolgáltatások, illetve interneten elérhető online adminisztrációs felületek felhasználó nevek / jelszavak biztonságos kezeléséért felhasználó a felelős. 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 Apagyi Zrínyi Ilona Általános 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.

Szerver biztonsági szabályzat

A szabályzat célja, hogy az intézmény 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.

A szabályzat vonatkozik minden, az Apagyi Zrínyi Ilona Általános Iskola tulajdonában, illetve felügyelete alatt levő szerverre.

Bejegyzetlen szerver nem működhet a iskola hálózatán.

A szervereknek illetéktelen behatolástól jól védettnek kell lennie, a szerverekhez való hozzáférést fizikailag is korlátozni kell.

A szervereken le kell tiltani minden nem használt szolgáltatást.

A szerverek konzoljairól az adminisztrációs tevékenység befejeztével ki kell lépni, nem szabad felügyelet nélkül bejelentkezve hagyni.

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.

Vírusvédelmi szabályzat

A számítógépes vírusok a számítógépen tárolt adatok és programok kártevői. A vírus a megfertőzött program futása közben másolja, többszörözi önmagát. 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.

A szabályzat ezen része a káros hatások megelőzésére, és a vírusfertőzés esetén elvégzendő teendők leírására szolgál.

A szabályzat hatálya

A vírusvédelmi szabályzat minden az iskola hálózatába kötött, ahhoz csatlakoztatott minden infokommunikációs eszközre vonatkozik.

Vírusvédelmi teendők

Vírusvédelmi szoftvert kell használni. Biztosítani kell a munkaállomások vírusvédelmét.

A vírusvédelmi programnak lehetőség szerint rezidens módban kell futnia, így az minden egyes rendszerindításkor aktivizálódik, és állandó háttérvédelmet biztosít.

A rendszergazdának meghatározott időnként minden gépen teljes vírusellenőrzést kell végrehajtania.

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 használat előtt vírusellenőrzést kell végezni.

Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.

A fontos adatokról és a rendszerkonfigurációról készüljön archiválás.

Teendők vírusfertőzés esetén

Tájékoztatni kell a vírusvédelemért felelős személyt (Digitális kultúra tanárt, rendszergazdát) a fertőzésről vagy annak gyanújáról.

Ha 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.

Az informatika terem használatával kapcsolatos szabályok

1. Az informatika terembe csak tanári engedéllyel és tanári felügyelettel lehet belépni.
2. Mindig fegyelmezetten kell viselkedni, ügyelve a gépteremben található eszközök épségére.
3. A terembe csak a füzetet és az íróeszközöket lehet bevinni! Táskát, kabátot az osztályteremben kell hagyni.
4. Ételt és italt a terembe bevinni és ott fogyasztani TILOS (csokit, rágót vagy gyümölcsöt sem)! A számítógép érzékeny berendezés, ezért különösen ügyelj környezetének rendjére és tisztaságára.
5. Adathordozót, vagy egyéb vírusterjesztésre alkalmas eszközt a gépterembe bevinni nem szabad. A gyerekeknek a számítógéphez csatlakozó vezetékekhez hozzányúlni, azokat kihúzni TILOS és balesetveszélyes.
6. A számítógépeket bekapcsolni, kikapcsolni, a hálózatba bejelentkezni csak tanári engedéllyel szabad.
7. Minden gyermek a létrehozott mappájába dolgozzon, a beazonosíthatatlan mappákat fájlokat időközönként töröljük.
8. Ügyeljünk arra, hogy a gyerekek ne változtassák meg az asztali ikonok nevét, az asztal hátterét, az egérmutató formáját stb. Ha átállította valaki, akkor állítsa vissza az eredeti nevére. Ha ilyet tapasztalsz, szólj, mert vissza tudjuk követni az órarend alapján, hogy ki ült az adott helyen.
9. Ne töltsenek le játékokat a gyerekek.
11. Az órák között, illetve a nap végén minden gépet ki kell kapcsolni és az ablakokat ellenőrizni, be vannak-e csukva, a klímaberendezést lezárni.
12. Kifogásolható tartalmú oldalak az Interneten nem látogathatók.
13. Tilos a szerzői jogok megsértése.
14. Szándékos károkozás esetén, az okozónak a kárt meg kell térítenie.
15. A teremben tüzet oltani csak porral oltó készülékkel szabad.

A tiltott és használatban korlátozott tárgyakra vonatkozó további szabályok

A 245/2024. (VIII. 8.) Korm. rendelet a nevelési-oktatási intézményekben a tiltott és a használatban korlátozott tárgyak köréről, valamint a tárgyakra vonatkozó eljárásrend részletes szabályairól szóló leirat alapján alapszabályainkba rögzítettük a tudnivalókat.

Amennyiben a tanuló információtechnológiai eszközt (okostelefon, okosóra) hoz be az intézménybe, azt le kell adni a következő módon:

1. óra előtt az osztályok az eszközöket a kijelölt dobozba teszik. Az osztályfőnök, vagy a megbízott pedagógus a dobozt elhelyezi tanári szobában elhelyezett kulcsos szekrénybe.

Az osztályfőnök, vagy a megbízott pedagógus az utolsó órája előtt felveszi az osztály dobozát a tanári szobából. A tanóra végén a tanuló elveszi a dobozból a saját információtechnológiai eszközét. Az osztályfőnök, vagy a megbízott pedagógus a dobozt visszahelyezi a tanári szoba kulcsos szekrényébe.

A tanulószobás gyerekek a tanulószobát vezető pedagógusnak adják le az eszközöket és a pedagógus gondoskodik az eszközök elzárásáról.

Sportkör, edzések esetén a tanulók leadják a tornaterem szertárába az eszközeiket, ahol a testnevelő elzárja a információtechnológiai eszközöket.

Ha a tanuló tiltott tárgyat vagy a használatban korlátozott tárgyat engedély nélkül birtokában tartja a tanítás időtartama alatt, azt a tanulótól a pedagógus átveszi. A pedagógus az eszközt az iskolavezetésnek átadja. Az eszközt csak a szülő/törvényes képviselő veheti át, munkanapokon 14:30-ig.

Ha a tanuló második alkalommal is megszegi a szabályzatban foglaltakat osztályfőnöki figyelmeztetésben részesül.

Apagy, 2024. szeptember 02.

