Török János Mezőgazdasági és Egészségügyi Szakgimnázium és Szakközépiskola

Informatikai biztonsági és szoftver szabályzat

2020

Tartalomjegyzék

Biztonsági osztály **4**

Általános rendelkezések **4**

Az Informatikai Biztonsági Szabályzat célja 4

Az alapul vett irányelvek, követendő szabványok, ajánlások **5**

A szabályzat felülvizsgálatának rendje, hatálya **6**

Az IBSZ hatálya **6**

Az IBSZ területi hatálya 6

Az IBSZ személyi hatálya 6

Az IBSZ tárgyi hatálya 6

Szabályozási elemek **7**

Informatikai biztonsági útmutató – IBU 7

Eszközökkel kapcsolatos szabályok 7

Jelszókezeléssel kapcsolatos szabályok 7

Szoftverekkel kapcsolatos szabályok 7

Adatvédelmi szabályok 7

Internethasználattal kapcsolatos szabályok 8

Vírusvédelmi szabályok 8

Szerepkörök **8**

Szerepkörök és felelősségek kialakítása 8

Rendszergazda 8

A rendszergazda felelőssége 9

A rendszergazda feladatai 9

A végfelhasználó felelőssége 9

Informatikai biztonsági rendelkezések **10**

Jogosultságkezelés 10

Jogosultságkezelés célja 10

Jogosultságkezelés folyamat lépései 10

Jelszókezelés követelményei 10

Az informatikai eszközök biztonsága 11

Fizikai védelem és környezet védelme 11

Területek védelme, biztosítása 11

Berendezések védelme 11

Berendezések karbantartása 12
Berendezések biztonságos selejtezése, illetve újrafelhasználása 12
Vagyontárgyak eltávolítása 12
Mozgatható perifériák és adathordozók kezelése 12
Adathordozók kezelése 12
Az eltávolítható adathordozók kezelése 12
Adathordozók selejtezése 12
Adathordozók biztonsági tárolása 12
Vírusvédelem 13
Segédeszközök 13
Használati előírások 13
Levelezés 13
Használati előírások 13
A szervezet elektronikus hivatalos kommunikációja 14
Internet használat 15
Szoftver védelem 15
Programhoz való hozzáférés, programvédelem 15
Programok fizikai védelme 15
Hardver védelem 15
Informatika, és egyéb tantermek rendje 17
Nyomtató és fénymásoló használat 17
Könyvtár 17
Gazdasági 18
Tanári 18
Nyilvános munkaállomások 18
Pazarló erőforrás használat 18
Szankciók 19
Műszaki alapfogalmak 19
Szervezeti egységek védelmi eszközei és módszerei 20
Tűzvédelem 20
Vagyonvédelem, fizikai biztonság 20

Biztonsági osztály

A 2013. évi L. törvény és az ide vonatkozó 77/2013. (XII. 19.) NFM rendelet előírásának megfelelően az iskola 1. biztonsági osztályba tartozik.

Általános rendelkezések

Az Informatikai Biztonsági Szabályzat célja

A jelen Informatikai Biztonsági Szabályzat (a továbbiakban IBSZ) célja, hogy a Török János Mezőgazdasági és Egészségügyi Szakgimnázium és Szakközépiskolánál működtetett informatikai rendszerre vonatkozóan a biztonsági intézkedéseket szabályozza, meghatározza a számítástechnikai eszközök beszerzésének és használatának, a szoftverkészítés és alkalmazás, az adatkezelés folyamatának biztonsági szabályait, továbbá az informatikai szerepköröket, és előírja az egyes szereplők informatikai biztonságot érintő feladatait.

Az IBSZ által biztosítható:

- A titok-, vagyon- és tűzvédelemre vonatkozó előírások betartása.
- A személyiségi jogok kellő védelme.
- Az üzemeltetett számítástechnikai eszközök, hardverek, szoftverek, hálózatok, stb. rendeltetésszerű használata és megfelelő üzemvitele.
- Az üzembiztonságot szolgáló műszaki fenntartás és karbantartási teendők elvégzése.
- A számítógépes feldolgozások és az eredményadatok további hasznosítása során az illetéktelen hozzáférésből és felhasználásból eredő károk megelőzése, illetve minimális mértékűre való csökkentése.
- Az adatállományok formai és tartalmi helyességének és épségének megőrzése.
- Az alkalmazott szoftverek sértetlenségének, megbízható működésének biztosítása
- Az adatállományok biztonságos mentése.
- A felhasznált és keletkezett írásos dokumentumok megfelelő kezelésének biztosítása.
- Annak rögzítése, hogy mi az iskolavezető beosztású és az informatikai feladatokat irányító dolgozóinak a feladata, felelőssége és a jogköre az informatikai biztonság tekintetében.
- A jogosultság és a hozzáférés rendszerének dokumentált kialakítása.
- A célok elérése érdekében a védelemnek működnie kell az egyes rendszerelemek fennállásának teljes ciklusa alatt – a megtervezéstől az alkalmazáson (üzemeltetésen) keresztül a felszámolásukig, és az azt követően az elévülés, illetve a selejtezhetőség időtartama alatt.

Az alapul vett irányelvek, követendő szabványok, ajánlások

Az IBSZ mint az információvédelem szabályozásának elsődleges eszköze, a vállalat működési területén szükségszerűen a hatályos jogszabályok, szabványok, ajánlások előírásain alapul. Ezek jellemzően a következők:

1995. évi LXV. törvény. az államtitokról és a szolgálati titokról,

79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről,

43/1994. (III. 29.) Korm. rendelet a rejtjeltevékenységről,

1992. évi LXIII. törvény. a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról,

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról,

233/2001. (XII.10.) Korm. rendelet a közszolgálati jogviszonnyal összefüggő adatkezelésre és közszolgálati nyilvántartásra vonatkozó szabályokról,

7/2002. (III. 12.) BM rendelet a közszolgálati nyilvántartás egyes kérdéseiről,

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről.,

Tűzvédelmi Szabályzat,

A vagyonvédelemmel kapcsolatos rendelkezések,

Az informatikai rendszerekre vonatkozó szabványok, ajánlások (elsősorban a MeH ITB 12. ajánlása),

Az iskola tevékenységét a rá vonatkozó Szervezeti és Működési Szabályzat (a továbbiakban SZMSZ), valamint az ebből, a szakági utasításokból és a magasabb jogszabályokból levezetett ügyrendek, eljárásrendek és belső szabályzatok szabályozzák. A belső, helyi szabályozások kiadása az intézményvezető felelőssége.

A szabályzat felülvizsgálatának rendje, hatálya

A felülvizsgálatot, évente vagy ha a működés rendjében változás történik, el kell végezni.

Az IBSZ hatálya

Az IBSZ területi hatálya

Az IBSZ rendelkezésének teljes körű és értelemszerű alkalmazása az iskola egész területén kötelező.

Az IBSZ személyi hatálya

Kiterjed az iskola minden felhasználójára.

Az IBSZ tárgyi hatálya

kiterjed az iskola területén lévő:

- az iskola által használt, vagy általuk tárolt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is
- rendszerprogramokra és felhasználói programokra
- adathordozókra, azok tárolására és felhasználására
- az informatikai folyamatban szereplő valamennyi dokumentációra

Az IBSZ rendelkezéseit minden újonnan üzembe helyezett informatikai rendszer esetében teljes körűen alkalmazni kell.

Szabályozási elemek

Informatikai biztonsági útmutató - IBU

Felhasználói biztonsági szabályzat

Az iskola a munkavégzéshez megfelelő számítástechnikai hátteret biztosít, a biztosított eszközöket azonban kizárólag munkavégzés céljára lehet használni.

A biztosított eszközök az iskola tulajdonát képezik.

Eszközökkel kapcsolatos szabályok

- Amennyiben a felhasználó bármilyen biztonsági problémát vagy hibát észlel azonnal köteles értesíteni a rendszergazdát.
- Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.
- Tilos az eszközök közelében enni, inni, dohányozni.

Jelszókezeléssel kapcsolatos szabályok

- A felhasználó 3 havonta köteles jelszavait lecserélni.
- A jelszó minimum 8 karakter hosszú, (kicsi és nagy) betűket és számokat is kell tartalmaznia.
- A jelszó nem írható le semmilyen jól látható, vagy könnyen hozzáférhető helyre.
- Tilos a névre szóló jelszó kiadása más felhasználók számára.

Szoftverekkel kapcsolatos szabályok

- az iskola kizárólag jogtiszta szoftverekkel dolgozik.
- A jogtisztaság biztosítása a rendszergazda feladata, ezért tilos a rendszergazdán kívül bármely más felhasználónak bármilyen terjesztési engedéllyel (freeware, shareware, stb.) rendelkező szoftvert, az iskola tulajdonát képező számítógépre feltelepíteni. Szoftverek törlését is csak a rendszergazda végezheti el. Ez alól kivételt képeznek a víruskeresők, melyek fertőzés esetén jogosultak a számítógépről fájlokat törölni.

Adatvédelmi szabályok

- Az iskola elhagyása esetén a számítógépet zárolni kell a „Windows" + „L" billentyűk egyidejű lenyomásával
- A személyes munkához közvetlenül nem kapcsolódó állományok tárolása mind a munkaállomásokon, mind a szervereken nem engedélyezett.

Internethasználattal kapcsolatos szabályok

- Tilos az iskolai internet kapcsolaton keresztül minden olyan program és egyéb fájl letöltése, ami nem a munkavégzéshez szükséges.
- Tilos minden internetes „online" sugárzott műsor (ide tartoznak a rádió, televízió műsorok) hallgatása, megtekintése az internet sávszélesség indokolatlan csökkentése miatt.
- Mindenféle fájlmegosztó alkalmazás használata az iskola számítástechnikai eszközein tiltott.

Vírusvédelmi szabályok

- A számítógépen vírusellenőrző program fut, mely a gép működése közben automatikusan figyeli a rendszert. A vírusellenőrző programot leállítani és annak működésébe beavatkozni szigorúan tilos.
- Minden fájlművelet előtt ez a program ellenőrzi a megnyitott fájlokat. Bármilyen, adatbiztonságot veszélyeztető esemény figyelmeztetése jelenik meg a felhasználó monitorán, azonnal értesíteni kell a rendszergazdát, hogy a megfelelő lépésekkel megakadályozhassa a kártékony programok további fertőzéseit.
- Vírustalálat esetén a munkát azonnali hatállyal fel kell függeszteni, a számítógépet az hálózatról le kell választani és megkezdeni az okok feltárását és helyreállítását.

Szerepkörök

Szerepkörök és felelősségek kialakítása

A rendszergazda és a végfelhasználók szerepköreit és felelősségeit oly módon kell kialakítani, és ismertetni, hogy a rendszergazda és a felhasználók között el legyen különítve a hatáskör, a felelősségek és az iskola igényeinek kielégítéséért való felelősség tekintetében.

Rendszergazda

A rendszergazda számára több automatizált programcsomag áll rendelkezésre, amely segít a biztonság folyamatos szinten tartásában, a logok elemzésével a gyanús programok megkeresésében, stb.

A rendszergazda felelőssége

- Az iskolai környezetben a vírusellenőrző programok működésének beállítása a rendszergazda feladata és felelőssége, és a felhasználó nemhogy engedélyt, de lehetőséget sem kaphat a vírusvédelmi beállítások bármilyen módosítására.
- Kialakítja a rendszer biztonságát, a biztonságpolitikával összhangban.
- Követnie kell a megfelelő internetes fórumokat, a gyártó híreit, hogy minél előbb tudomást szerezzen az esetleges problémákról.
- A természetes tevékenységek, mint a rendszeres mentés és karbantartás is a rendszergazda feladata.

A rendszergazda feladatai

A rendszergazda feladata a hálózat és a hálózatban részt vevő egységek biztonságának megoldása, felügyelete, javaslatok megtétele a biztonsági hiányosságok pótlására. Felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért. Gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról. Feladata a védelmi eszközök működésének folyamatos ellenőrzése. Felelős az iskola informatikai rendszer hardver eszközeinek karbantartásáért. Gondoskodik a folyamatos vírusvédelemről. Folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását. Ellenőrzi a rendszer adminisztrációját.

A végfelhasználó felelőssége

Az eszközök kezelése, használata során minden felhasználónak gondosan be kell tartani az alábbiakat:

- Minden olyan előírást, mely az eszközök kezelési útmutatójában szerepel.
- A szoftverek, dokumentumok használata, létrehozása során a szerzői jogokra vonatkozó jogszabályokat.
- A munka és tűzvédelmi előírásokat, szabályokat
- Tilos az eszközök közelében ételt, italt fogyasztani, tárolni.
- Tilos a géptermek teljes területén élelmiszert fogyasztani, vagy azokat kicsomagolt állapotban tartani.
- Tilos az eszközöket és azok részeit áthelyezni, mozgatni, burkolatukat, csatlakozásaikat megbontani.
- Tilos a számítógépekre szoftvert telepíteni, illetve engedély nélkül eltávolítani.
- Tilos a rendszergazda engedélye nélkül külső programot futtatni.
- Tilos illegális vagy bármilyen jogszabályba ütköző tevékenységet folytatni.

- Tilos a telepített szoftverek konfigurációját és az operációs rendszer beállításait megváltoztatni.

Informatikai biztonsági rendelkezések

Jogosultságkezelés

Jogosultságkezelés célja

Azonosító - Minden egyes felhasználónak saját személyes és kizárólagos használatára szóló egyedi azonosítóval (felhasználó ID) kell rendelkeznie.

Jelszó - „Valami, amit tudunk" Egy olyan egyedi karaktersorozat, amely az adott azonosítóval párosítva egyértelműen alkalmas a felhasználó azonosítására, és megfelel a jelszóval szemben támasztott követelményeknek.

Jogosultságkezelés folyamat lépései

Felhasználói hozzáférés irányítása - Az első lépés mindig a felhasználó regisztrálása. Minden információs rendszerhez és azokon belül minden szolgáltatáshoz egy hivatalos regisztrálási eljárást kell kezdeményezni. Amennyiben a felhasználó regisztrálása megtörténik, úgy úgynevezett előjogokat és jelszavakat kell kiosztani a felhasználó számára, az előjogokat természetesen bizonyos időnként felül kell vizsgálni, a jelszavak kiosztását pedig folyamatosan felügyelni kell és a jogosultságokat időnként hivatalosan át kell vizsgálni. Amennyiben az alkalmazottnak megszűnik az alkalmazása, úgy a hozzáférésének jogosultságát meg kell szüntetni, változás esetén természetesen csak módosítani kell.

Felhasználói felelősségek - Azon túl, hogy szabályozzuk a felhasználók jogosultságait, minden a rendszerben regisztrált felhasználó felelősséggel tartozik a jelszavának védelméért, ehhez a következőket kell teljesíteni: A jelszóválasztásnál figyelembe kell venni, az azzal kapcsolatos alapvető biztonsági elvárásokat. A felhasználóktól meg kell követelni, hogy a jelszavak kiválasztásában és használatában a jó biztonság gyakorlatot kövessék. [ISO/IEC 27001 / A11.3.1] Védeni kell az őrizetlenül hagyott berendezéseket. A felhasználóknak biztosítaniuk kell az őrizetlenül hagyott berendezések megfelelő védelmét. [ISO/IEC 27001 / A11.3.2]

Jelszókezelés követelményei

- A kezdetben generált jelszót az első bejelentkezés alkalmával kötelezően meg kell változtatni.
- A jelszónak minden felhasználó számára bármikor szabadon megváltoztathatónak kell lennie.

- A választott jelszó összefüggő szövegként soha ne legyen olvasható.
- A jelszó és a hozzátartozó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezés során sem.
- A jelszó minimális hossza felhasználók esetében minimum 6 karakter, kiemeltebb jogosultság esetén 12 karakter hosszúnak kell lennie.
- A biztonságos jelszó kialakításánál, a kisbetűk, nagybetűk, számok és speciális karakterek csoportok közül legalább 3 fajta típust tartalmaznia kell a választott jelszónak.
- További feltétel, hogy nem tartalmazhatja a felhasználó nevét még részleteiben sem.
- A jelszó maximális élettartama felhasználók esetén 90 nap, míg adminisztrátorok esetén 30 nap.
- A jelszó egyediségét 3 ciklusra visszamenőleg ellenőrizni kell.
- Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte azonnal le kell azt cserélnie.
- A jelszó ne legyen kívülálló számára kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat.
- A jelszavakat nem szabad felírni, papíron tárolni, amennyiben az elkerülhetetlen (kezdetben generált jelszó esetén) gondoskodni kell a jelszó biztonságos helyen zárt borítékban történő tárolásáról.

Az informatikai eszközök biztonsága

Fizikai védelem és környezet védelme

A fizikai védelmi intézkedések az információ feldolgozását kiszolgáló berendezések, helyiségek és az alkalmazottak védelmét szolgálják. Ilyenek például a vagyonvédelmi, a tűzjelző-, a beléptető- és a videó meg-figyelő-rend-szerek vagy akár a szünetmentes áram-források, védett kábelrendezők, klíma berendezések.

Területek védelme, biztosítása

Cél: A szervezet helyiségeinek és információinak védelme, a jogosulatlan, illetéktelen fizikai behatolás, károkozás és zavarkeltés megakadályozása.

Berendezések védelme

Cél: A vagyontárgyak elvesztésének, károsodásának, eltulajdonításának, illetve megrongálásának, valamint a szervezeti működés fennakadásának megelőzése.

A berendezéseket úgy kell elhelyezni, illetve védeni, hogy csökkenjen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége.

Berendezések karbantartása

A berendezéseket előírásszerűen karban kell tartani folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében.

Berendezések biztonságos selejtezése, illetve újrafelhasználása

Valamennyi olyan berendezést, amely tárolóeszközt foglal magában, ellenőrizni kell annak biztosítása érdekében, hogy az érzékeny adatok és engedélyezett szoftverek a selejtezést megelőzően eltávolításra, illetve biztonságos felülírásra kerüljenek.

Vagyontárgyak eltávolítása

Berendezések, információk, illetve szoftverek előzetes engedély nélkül nem vihetők ki az iskolából.

Mozgatható perifériák és adathordozók kezelése

Adathordozók kezelése

Cél: Vagyontárgyak illetéktelen kiadásának, módosításának, eltávolításának, vagy tönkretételének, valamint a működési tevékenységek megszakadásának megelőzése.

Az eltávolítható adathordozók kezelése

Intézkedés: Az eltávolítható adathordozók kezelésére megfelelő eljárásokat kell alkalmazni.

Adathordozók selejtezése

Intézkedés: A feleslegessé vált adathordozókat hivatalos eljárásokkal védett módon és biztonságban le kell selejtezni, vagy meg kell semmisíteni.

Adathordozók biztonsági tárolása

Az üzletmenet szempontjából alapvető fontosságú informatikai rendszerek adatait tervezett módon, rendszeresen olyan biztonsági adathordozókra kell menteni, amelyekről egy esetleges

üzemzavar esetén egy utolsó, működőképes állapotot vissza lehet állítani. A biztonság érdekében a mentések egyik példányát az informatikai központtól távol kell elhelyezni.

Vírusvédelem

A célkitűzés az, hogy megvédjük az adatok sértetlenségét a szoftvereknek és az adatoknak.

A vírusvédelem egy megelőző tevékenység a legtöbb esetben, segítségével megelőzhetőek a rosszindulatú kódok és a jogosulatlan mobil kódok futtatása.

Segédeszközök

Minden az iskola tulajdonában lévő számítógépen telepítve kell lennie az iskola által engedélyezett vírusvédelmi szoftver valamelyikének.

Windows XP esetén: ESET Endpoint Antivius

Windows 7 esetén : ESET Endpoint Antivirus

Használati előírások

- A vírusvédelmi szoftvereket naprakészen kell tartani, mindig az elérhető legújabb stabil verziót kell feltelepíteni.
- A vírusvédelmi szoftvert sosem szabad kikapcsolni.
- Minden fájlt ellenőrizni kell a használat előtt, amelyet elektronikus vagy optikai adathordozóról szeretnénk használni vagy a hálózaton keresztül szereztünk be.
- Ellenőrizni kell az e-mail csatolmányait és a letöltött állományokat mielőtt használnánk azokat.

Levelezés

Használati előírások

A felhasználóknak külön figyelniük kell a nem megbízható csatolmányokra, amelyek nem megbízható forrásból származnak.

A felhasználók nem adhatják ki magukat másnak levelezés közben.

A levelek helyesen és professzionálisan legyenek megfogalmazva, ne tartalmazzanak rágalmazó, sértő tartalmat.

A szervezet elektronikus hivatalos kommunikációja

A hivatalos elektronikus kommunikáció elsősorban kormányzati e-mail címek igénybevétele útján folyhat.

Kormányzati e-mail címnek kell tekinteni:

a) a gov.hu végződésű e-mail címeket,
b) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv által biztosított hivatalos elektronikus levelezési címeket,
c) a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket,
d) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv vagy a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alatt álló gazdasági társaság tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket, valamint
e) a Kormány irányítása vagy felügyelete alá nem tartozó, Alaptörvényben meghatározott szerv hivatalos elektronikus levelezési címeit.

Kizárólag kormányzati e-mail címre küldhetők ki a továbbiakban az alábbi iratok:

- törvényjavaslatot tartalmazó irat,
- Kormány részére készült előterjesztés, jelentés,
- Kormány döntését igénylő előterjesztés,
- politikai felsővezetői (miniszterelnök, miniszter, államtitkár) döntést igénylő előterjesztés, különösen miniszteri rendelettervezet,
- politikai felsővezető részére készülő előterjesztés, jelentés,
- politikai vezető (kormánymegbízott) részére készülő előterjesztés, jelentés,
- biztosi jogviszonyban álló (kormánybiztos, miniszterelnöki biztos, miniszteri biztos) részére készülő előterjesztés, jelentés,
- szakmai felsővezető (közigazgatási államtitkár, helyettes államtitkár, központi hivatal vezetője és vezetőjének helyettese, kormányhivatal főigazgatója) részére készülő előterjesztés, jelentés
- szakmai vezető (kormányhivatal igazgatója, járási hivatal, illetve fővárosi kerületi hivatal vezetője és vezetőjének helyettese, főosztályvezető, osztályvezető) részére készülő előterjesztés, jelentés,
- minden olyan irat, amely a Kormánynak, a Kormány tagjának, politikai felsővezetőnek vagy vezetőnek, szakmai vezetőnek vagy felsővezetőnek, biztosi jogviszonyban állónak a döntését tartalmazza, mely nem kerül nyilvánosan közzétételre,
- a fentiekről készült tervezet, másolat vagy kivonat, a fentiekkel kapcsolatos munkaanyag

Ezen irattípusok nem kormányzati e-mail címre történő kiküldése tilos, kivéve, ha azt az Ön szervezetében erre kijelölt vezető kifejezetten, írásban (ez alatt az elektronikus jóváhagyást is érteni kell) engedélyezi. Az erre kijelölt vezető felelősségi körébe tartozik annak mérlegelése, hogy a fenti irattípusok közé tartozó irat nem kormányzati e-mail címre történő továbbítása nem eredményezi-e a dokumentum illetéktelen kezekbe kerülését. (Javaslom, hogy a nem-kormányzati e-mail címmel rendelkező címzett részére rendszeresen megküldendő anyag

tekintetében elegendő legyen egyszer kérni az engedélyt, erre az engedélykérés során szükséges legyen utalni.)

Amennyiben a fenti irattípusok közé tartozó irat nem-kormányzati e-mail címre történő továbbítására engedély nélkül kerül sor, akkor annak minden esetben munkajogi következményekkel kell járnia az intézkedésben részt vevő kollegák irányában.

Amennyiben a fentiek szerinti irat nem kormányzati e-mail címre történő megküldése szükséges, akkor az irat továbbítása helyett elsősorban az irat tartalmának kivonatolása útján kell az abban foglaltakat a címzettel közölni. Ennek során lehetőleg kerülni szükséges az utalást arra, hogy a kérdéses tartalom végső soron honnan származik és azt milyen dokumentum tartalmazza, ehelyett elsősorban általános körülírással szükséges utalni a dokumentumban foglaltak keletkeztetőjére.

Internet használat

- bármilyen hiba vagy probléma előfordulása esetén a dolgozó első feladata értesíteni a Rendszergazdát
- Tilos sértő tartalmak letöltése, fenyegetés és erőszakos fellépés, illegális tevékenységek

Szoftver védelem

Az üzemeltetésért felelős dolgozónak biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

Programok fizikai védelme

- A védelem érdekében a felhasználás helyétől elkülönítve kell tárolni

Hardver védelem

- a számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől

- a számítógép közelében ételt és italt fogyasztani tilos
- fali csatlakozók megbontása szigorúan tilos
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak
- a számítógép belsejébe nyúlni, és ott bárminemű változtatást okozni tilos. csak az illetékes szakember, illetve a szervizek szakemberei nyúlhatnak bele

Informatika, és egyéb tantermek rendje

- Az elsődleges felelős a mindenkori felügyelő tanár vagy helyettesítője! Az iskola rendszergazdája bármikor, előre nem egyeztetett időpontban ellenőrizheti az eszközöket a munka zavartalanságának figyelembevételével.
- Tilos a tanulókat felügyelet nélkül hagyni (a tanár vagy helyettesítője egy pillanatra sem hagyhatja magára a tanulót a tanteremben)!
- A tanár vagy helyettesítője csak utoljára hagyhatja el a tantermet, nem bízhat meg mást a terem felügyeletével.
- A tanár vagy helyettesítője köteles figyelemmel követni a tanulók cselekedeteit.
- Azt a tanulót, aki a munkában előrehaladt, nem jogosítja fel arra, hogy bármit csinálhat, bármilyen eszközt használhat.
- Tilos a számítógépeken az aktuális tananyaghoz nem kapcsolódó szoftvert futtatni.!
- A tanárnak kötelessége a tanulók internet használatát figyelni.!
- A tantermekben szigorúan csak a tananyaghoz kapcsolódó tartalmakat szabad letölteni, melyek éppen az aktuális munkafolyamathoz szükségesek.
- Tilos az eszközök közelében ételt és italt fogyasztani!
- Tilos az eszközöket mozgatni, csatlakozót, burkolatot megbontani!
- Tilos külső vagy belső eszközöket engedély nélkül csatlakoztatni, eltávolítani!

Nyomtató és fénymásoló használat

Az irodákban elhelyezett nyomtatók és fénymásolók használata csak a tanórához szükséges dokumentumok és az adminisztratív munkák nyomtatására és másolására engedélyezett.

Könyvtár

- A könyvtárban lévő számítógépekért a könyvtáros a felelős!
- A könyvtárban lévő számítógépekre a könyvtáros engedélyével lehet Pen Drive-ot csatlakoztatni
- Az internetet a könyvtáros engedélyével lehet használni.
- A könyvtár rendelkezik egy saját könyvtár adminisztratív munkáihoz szükséges számítógéppel, amit csak a könyvtáros használhat.
- Tilos a számítógépekre a rendszergazda engedélye nélkül telepíteni vagy azokról eltávolítani programot!
- Tilos az eszközök közelében ételt, italt tartani, fogyasztani!
- Tilos az eszközöket mozgatni, csatlakozót, burkolatot megbontani!
- Tilos külső vagy belső eszközöket engedély nélkül csatlakoztatni, eltávolítani!

Gazdasági

- Az irodákban található számítógépeket, csak az ott dolgozók használhatják.
- Tilos a számítógépekre a rendszergazda engedélye nélkül telepíteni vagy azokról eltávolítani programot!
- Tilos az eszközök közelében ételt, italt tartani, fogyasztani!
- Tilos az eszközöket mozgatni, csatlakozót, burkolatot megbontani!
- Tilos külső vagy belső eszközöket engedély nélkül csatlakoztatni, eltávolítani!

Tanári

A tanáriban elhelyezett számítógépeket az iskolában dolgozó pedagógusok használhatják.

- Tilos a számítógépekre a rendszergazda engedélye nélkül telepíteni vagy azokról eltávolítani programot!
- Tilos az eszközök közelében ételt, italt tartani, fogyasztani!
- Tilos az eszközöket mozgatni, csatlakozót, burkolatot megbontani!
- Tilos külső vagy belső eszközöket engedély nélkül csatlakoztatni, eltávolítani!

Nyilvános munkaállomások

A zsibongóban elhelyezett számítógépeket kizárólag informálódás céljából használhatóak!

- Tilos a számítógépekre a rendszergazda engedélye nélkül telepíteni vagy azokról eltávolítani programot!
- Tilos az eszközök közelében ételt, italt tartani, fogyasztani!
- Tilos az eszközöket mozgatni, csatlakozót, burkolatot megbontani!

Pazarló erőforrás használat

Az erőforrást itt a lehető legtágabban értelmezzük: emberi és fizikai erőforrást egyaránt értünk alatta. Erőforrásnak tekintjük a felhasználók, rendszergazdák idejét, munkáját, a számítógépek memória- és diszkterületeit, a számítási kapacitásaikat, a kommunikációs csatornák

sávszélességét stb. Ezért mindenki ezeket az erőforrásokat meggondoltan használja, ügyeljen elkerülni a pazarlást.

Szankciók

Az rendszergazda bármikor jogosult ellenőrizni az iskola eszközeinek szabályos használatát. Az ellenőrzés tényét nem köteles előre bejelenteni, de törekednie kell, hogy az ne zavarja feleslegesen a napi munkamenetet.

Ha felhasználó az intézmény eszközeit nem a szabályzat előírásainak megfelelően használja, úgy fegyelmi vétséget követ el. A szabályok megszegése esetén a jogosultság megvonható, illetve a minimális szintre csökkenthető. A jogosultság megvonása az elkövetett szabálytalanság függvényében lehet ideiglenes, vagy végleges. A rendszergazda az általa hozott korlátozó intézkedéseket a számítógéprendszer üzemeltetőjének (iskola igazgatójának) jelenti, aki dönt annak jóváhagyásáról, illetve a továbbiakban szükséges intézkedésekről.

Mivel a szabályok megszegése az egész iskola informatikai rendszerének, s így mások munkájának biztonságát is veszélyeztetheti, ezért a rendszergazda indokolt esetben saját hatáskörében akár azonnali kitiltást is alkalmazhat. A korlátozó intézkedések ellen az intézményvezetőnél lehet panasszal élni.

Amennyiben az elkövetett vétség a Büntető Törvénykönyv szerint bűncselekménynek minősül, úgy a rendszergazda a tudomására jutást követően azonnal köteles teljes kitiltást foganatosítani, a felhasználó adatait zárolni, s az intézmény vezetőjének a cselekményt jelenteni.

A felhasználó minden olyan általa okozott kárért teljes körű kártérítési kötelezettséggel tartozik, mely az eszközök rendeltetés vagy előírás szerinti használatának megszegése miatt.

Műszaki alapfogalmak

- szerver: olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza
- munkaállomás: egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál
- gépterem: az a helyiség, ahol az iskola tanulói és dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz
- adat: a tények, az elképzelések nem értelmezett, de értelmezhető közlési formája

- adatállomány: valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz
- adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere
- adatfeldolgozás: az adatok gyűjtése, rendszerezése, törlése, archiválása
- adatvédelem: az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik
- alkalmazói program (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be és amely a hardver és az üzemi rendszer funkcióit használja
- felhasználó: az a személy vagy szervezet, aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához
- hardver: az informatikai rendszer eszközeit, fizikai elemeit alkotó részei
- hálózat: két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé
- informatikai biztonság: olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni
- rendszerprogram (rendszer szoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják

Szervezeti egységek védelmi eszközei és módszerei

Tűzvédelem

A gépterem a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

Vagyonvédelem, fizikai biztonság

- a gépterembe való be- és kilépés rendjét szabályozni kell
- munkaidőn túl a gépteremben csak engedéllyel lehet tartózkodni
- a gépterembe történő illetéktelen behatolás tényét azonnal jelenteni kell
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt dolgozók használhatják

- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős

Ennek a szabályzatnak a nem ismerése, nem mentesíti a felhasználót a megsértése esetén foganatosítható szankciók, illetve az esetleges büntetőjogi következmények alól! A szabályzat bármely pontjának nem betartása súlyos fegyelmi vétségnek minősül!

Cegléd, 2020. április 16.

P.H.

Bácskai József
igazgató

Megismerési záradék

Alulírottak nyilatkozunk arról, hogy az Intézmény Informatikai biztonsági és szoftver Szabályzatát megismertük, azt a saját feladatunk vonatkozásában magunkra nézve kötelezőnek ismerjük el.

Név	*Munkakör*	*Aláírás*	*Dátum*
Kataticsné Vezsenyi Erika	gazdasági vezető		2020.04.16
Bicskei Károly	igazgató-helyettes		2020.04.16
Tóthné Czeróczki Mónika	igazgató-helyettes		2020.04.16
Práger Katalin	könyvelő		2020.04.16
Kisné Kerekes Hajnalka	munkaügyi előadó		2020.04.16
Ondavai Csaba	tangazdaság vezető		2020.04.16
Oláhné Kiszel Edit	gyakorlati oktatás vezető		2020.04.16
Bíró Tamás	rendszergazda		2020.04.16

A megismertetési feladatokat a mai napon elláttam

Kelt: 2020. 04. 16.

Ph.

Török János Mezőgazdasági és Egészségügyi Szakgimnázium és Szakközépiskola Cegléd 6.

.....

megismertető aláírása
(munkaköre: igazgató
neve: Bácskai József)