Szegedi SZC Déri Miksa Műszaki Technikum

Informatikai Biztonsági Szabályzat

2024.

Tartalom

1. Általános rendelkezések

1.1. Az Informatikai Biztonsági Szabályzat célja

A jelen Informatikai Biztonsági Szabályzat (a továbbiakban IBSZ) célja, hogy Szegedi SZC Déri Miksa Műszaki Technikumban 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 azinformatikai 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.

2. Irányelvek, követendő szabványok, ajánlások

Az IBSZ, mint az információvédelem szabályozásának elsődleges eszköze, az intézmény 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 szakágú utasításokból és a magasabb jogszabályokból levezetett ügyrendek, eljárásrendek és belső szabályzatok szabályozzák. A belső, helyi szabályozások kiadása az intézményvezető felelőssége.

3. A szabályzat felülvizsgálatának rendje, hatálya

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

4. Az IBSZ hatálya

4.1. Az IBSZ területi hatálya

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

4.2. Az IBSZ személyi hatálya

Kiterjed az iskola minden felhasználójára.

4.3. 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 teljeskörűen alkalmazni kell.

5. Szabályozási elemek

5.1. 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.

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 rendszergazda végezheti el.

Wifivel kapcsolatos szabályok

- Iskolánkban a belső hálózatára, a rendszergazda engedélye nélkül, tilos bármilyen wifi eszközt csatlakoztatni.

- Az intézményükben működő DM-AP, valamint az eduroam wifi kapcsolódási pontokat kizárólag az iskolánkban dolgozó személyek használhatják. Tanulóknak csatlakozni ezekre a hálózatokra tilos.
- A GUEST_vendég wifi hálózat szolgál az ideiglenesen az iskolában tartózkodók, valamint az iskolánkban tanuló diákok kiszolgálására. A hálózat jelszóval védett, melyhez hozzáférést a rendszergazda biztosít.

Adatvédelmi szabályok

- Az iskola elhagyása esetén a számítógépet zárolni kell.
- A személyes munkához közvetlenül nem kapcsolódó állományok tárolása mind a munkaállomásokon, mind a szervereken nem engedélyezett.

Internethasználattal kapcsolatos szabály

- Tilos az iskolai internetkapcsolaton keresztül minden olyan program és egyéb fájl letöltése, ami nem a munkavégzéshez szükséges.

6. Szerepkörök

6.1. 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.

A rendszergazda feladata, felelőssége

- Kialakítja a rendszer biztonságát a biztonságpolitikával összhangban.
- Követnie kell a megfelelő internetes fórumokat, a gyártók híreit, hogy naprakész információval rendelkezhessen.
- A természetes tevékenységek, mint a rendszeres mentés és karbantartás is 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 újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról.
- Feladata a védelmi eszközök működésének folyamatos ellenőrzése.
- Felelős az iskola informatikai rendszer hardvereszközeinek karbantartásáért.
- 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 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.

7. Informatikai biztonsági rendelkezések

7.1. Jogosultságkezelés

Jogosultságkezelés célja

Azonosító

Minden egyes felhasználónak saját személyes és kizárólagos használatára szóló egyedi azonosítóval kell rendelkeznie.

Jelszó

Egy olyan egyedi karaktersorozat, mely az adott azonosítóval párosítva egyértelműen alkalmas a felhasználó azonosítására.

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. Amennyiben az alkalmazottnak megszűnik az alkalmazása, úgy a hozzáférésének jogosultságát meg kell szüntetni, változás esetén természetesen csak módosítani kell.

Felhasználó felelősségek

Azon túl, hogy szabályozzuk a felhasználók jogosultságait, minden, a rendszerben regisztrált felhasználó felelősséggel tartozik jelszavának védelméért.

Jelszókezelés követelményei

- A jelszónak minden felhasználó számára bármikor szabadon megváltoztathatónak kell lennie.
- A jelszó és a hozzá tartozó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezés során sem.
- A jelszó minimális hossza felhasználók esetében legalább 6 karakter, kiemeltebb jogosultság esetén 12 karakter hosszúnak kell lennie.

- A biztonságos jelszó kialakításánál a kisbetűs, nagybetűs, szám és speciális karaktercsoportok közül legalább 3 fajta típust tartalmaznia kell.
- További feltétel, hogy nem tartalmazhatja a felhasználó nevét még részleteiben sem.
- 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 ez elkerülhetetlen, gondoskodni kell a jelszó biztonságos helyen zárt borítékban történő tárolásáról.

7.2. 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- és a videómegfigyelő rendszerek, vagy akár a szünetmentes áramforrások, védett kábelrendezők, klímaberendezések.

Területek védelme, biztosítása

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

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 biztonsága 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.

7.3. 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.
Abiztonság érdekében a mentések egyik példányát az informatikai központtól távol kell elhelyezni.

7.4. 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, professzionálisan legyenek megforgalmazva, ne tartalmazzanak rágalmazó, sértő tartalmat.

A Fenntartó elvárásainak megfelelően az intézmény kormányzati e-mailek fogadására alkalmas fiókot létesített. A kormányzati e-mail címről érkező levelek, iratok más e-mailre történő továbbküldése, csak indokolt esetben és csak az ezért felelős személy írásos engedélyével vagy elektronikus jóváhagyásával történhet. Minden egyéb esetben ezek továbbküldésük tilos.

Internet használat
- Bármilyen hiba vagy probléma előfordulása esetén a dolgozó első feladata értesítenia rendszergazdát.
- Tilos a sértő tartalmak letöltése, online fenyegetés és erőszakos online fellépés vagy más illegális tevékenység.

Szoftvervédelem
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, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a programdokumentációt.

Programok fizikai védelme

- A védelem érdekében a felhasználás helyétől elkülönítve kell tárolni.

Hardvervédelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől.
- 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 szervizek szakemberei nyúlhatnak bele.

8. Informatika és egyéb tantermek rendje

- Az elsődleges felelős a mindenkori felügyelőtanár vagy helyettesítője! Az iskola rendszergazdája bármikor, előre nem egyeztetett időpontban ellenőrizheti az eszközöket a munka zavartalanságának figyelembevételével.
- Tilos a tanulókat felügyelet nélkül hagyni! Az oktató vagy helyettesítő egy pillanatrasem hagyhatja magára a tanulót a tanteremben.
- Az oktató vagy helyettesítője csak utoljára hagyhatja el a tantermet, nem bízhat meg mást a terem felügyeletével.
- Az oktató 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.
- Az oktató kötelessége a tanulók internethasználatát figyelni.
- A tantermekben szigorúan csak a tananyaghoz kapcsolódó tartalmakat szabad letölteni, melyek éppen az aktuális munkafolyamathoz szükségesek.
- Tilos az eszközök közelében ételt, italt fogyasztani!
- Tilos az eszközöket mozgatni, csatlakozót, burkolatot megbontani.
- Tilos külső vagy belső eszközöket engedély nélkül csatlakoztatni, eltávolítani.

8.1. Nyomtató és fénymásolóhasználat

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

8.2. Könyvtár

- A könyvtárban lévő számítógépekért a könyvtáros felelős!
- A könyvtárban lévő számítógépekre a könyvtáros engedélyével lehet adathordozót csatlakoztatni.
- 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.

8.3. Gazdasági iroda; Tanulmányi iroda

- 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.

8.4. Tanári szoba

- A tanáriban elhelyezett számítógépeket csak 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.

8.5. Pazarló erőforráshasználat

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 lemezterületeit, a számítási kapacitásaikat, a kommunikációs csatornák sávszélességét, stb. Ezért mindenki ezeket az erőforrásokat meggondoltan használja, ügyeljen elkerülni a pazarlást.

8.6. Szankciók

A 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 a felhasználó az intézmény eszközeit nem a szabályzat előírásainak megfelelően használja, úgy fegyelmi vétséget követ el. A szabályok megszegése esetén 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 teljeskörű kártérítési kötelezettséggel tartozik, mely az eszközök rendeltetés vagy előírásszerinti használatának megszegése miatt történt.

9. 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 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 része.
- 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, rendszerszoftver: olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

10. Szervezeti egységek védelmi eszközei és módszerei

10.1. Tűzvédelem

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

10.2. Vagyonvédelem, fizikai biztonság

- A gépterembe való be- és kilépés rendjét szabályozni kell.
- A 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.

11. Mentési terv

A mentési terv eljárás vagy tevékenység, lépések sorozata annak biztosítására, hogy az iskola kritikus információfeldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal katasztrófa után. A számítógépkatasztrófa egy olyan esemény, amely az adatfeldolgozó képesség elvesztését okozza hosszabb időre.

11.1. A mentési terv részei

- A mentési terv definíciója.
- A megelőzési terv.
- A helyreállítási terv.

A megelőzési terv azon lépések sorozata, amelyet azért hajtanak végre a katasztrófát megelőzően normál üzem során, hogy lehetővé tegyék a szervezet számára a reagálást a katasztrófára. A mentési terv biztosít elmentett eszközöket a helyreállításhoz.

Így például az optikai tároló sokkal könnyebbé teheti nagy tömegű papíralapú dokumentumok helyreállítását.
A helyreállítási terv eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy helyreállítsák az informatikai rendszert.

11.2. A helyreállítási terv négy szakasza

- Azonnali reakció: válasz a katasztrófahelyzetre, a veszteségek számbavétele, a megfelelő szakemberek értesítése és a katasztrófaállapot megállapítása.
- Környezeti helyreállítás: az adatfeldolgozó rendszer helyreállítása (operációs rendszerek, felhasználó programok).
- Funkcionális helyreállítás: az informatikai rendszer alkalmazásainak és adatainak helyreállítása.
- Az elvesztett vagy az újonnan keletkezett adatok ismételt bevitele: a rendszergazdaés a felhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet.

Az Informatikai Biztonsági Szabályzat nem ismerete nem mentesíti a felhasználót a megsértése esetén foganatosítható szankcióktól, illetve az esetleges büntetőjogi következmények alól! A szabályzat bármely pontjának nem betartása súlyos fegyelmi vétségnek minősül!

Szeged, 2024. március 07.

Szegedi SZC Déri Miksa Műszaki Technikum 6724 Szeged, Kálvária tér 7. 1.

.....
Kurusa József
igazgató