TÁNCSICS MIHÁLY
SZAKKÖZÉPISKOLA, SZAKISKOLA ÉS KOLLÉGIUM

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A dokumentumváltozat készítésének dátuma 2011.02.28.

1. sz. példány

Tartalom

1. Bevezetés

Ez az Informatikai Biztonsági Szabályzat (továbbiakban Szabályzat) a Táncsics Mihály Szakközépiskola, Szakiskola és Kollégium (*továbbiakban:* Középiskola) dolgozói és tanulói által használt informatikai rendszerek és eszközök működtetésének és használatának általános szabályait rögzíti.

Ebben a Szabályzatban a Táncsics Mihály Szakközépiskola, Szakiskola és Kollégium informatikai rendszerének működését biztonsági és adatvédelmi szempontból szabályozza.

Az Informatikai Biztonsági Szabályzat tartalmazza a Középiskola hozzáállását információ biztonságához, valamint az informatikai rendszereire specifikált részletes szabályozást.

A Szabályzat a Középiskola minőségirányítási rendszerével egységes szabályozást ad a Középiskola SZMSZ mellékleteként, a Középiskola Szervezeti és Működési Szabályzatának felhasználásával készült, rendelkezései kiterjednek a Középiskola szervezeti egységeire és munkatársaira.

A Szabályzatban előforduló informatikai kifejezések értelmezését a *Fogalmak, meghatározások, értelmezések* fejezetben adjuk meg.

2. A Középiskola informatikai rendszerének irányítása

2.1 Az informatikai biztonság koordinálása

A Középiskola a rá vonatkozó törvények, rendeletek stb. által meghatározott feladatai szerint oktató, de adat- és információ-gyűjtő, elemző és szolgáltató szervezet is. Feladatai megoldásában meghatározó mértékben támaszkodik a már kialakított és folyamatosan fejlődő informatikai rendszerre, és az ebben a keretben működő információs rendszerekre.

A kialakított informatikai rendszer alapvetően központosított, az információs rendszerek operatív működtetése az informatikai munkaközösség vezető (rendszergazda) szakmai irányítása és felügyelete mellett történik.

A Középiskola az egyéni eszközökre és a meghatározott biztonsági eljárások végrehajtására vonatkozó felelősségeket világosan meghatározza a munkaköri leírásokban, az eljárásokban, az SZMSZ-ben, a szabályozó belső utasításokban.

2.2 A Középiskola felhasználói csoportjainak informatikai vonatkozású tevékenységei

Az alábbi táblázat a Középiskola által felhasznált informatikai rendszereket tartalmazza

Felhasználói csoport	Feladat, amelyhez informatikai eszközt használ	Informatikai rendszer, vagy alkalmazás
A középiskola valamennyi felhasználója	Elektronikus levelezés, web böngészés, dokumentumkezelés	Windows, Thunderbird, Firefox, Word, Excel
Gazdasági iroda munkatársai	Pénzügyi gazdálkodási rendszer	IMI, Tanulónyilvántartás, Menza-nyilvántartás
Iskolai adminisztráció (vezetőség, adminisztratív dolgozók)		Tanulónyilvántartás (kliens modul), Tanuló nyilvántartó program
Tantestület tagjai	CAD oktatás	AutoCAD, NetSupport School, CorelDraw, PowerPoint
Tanulók, akiknek a tanulói jogviszonya fennáll		PowerPoint, Access CNC szimuláció, Weblapszerkesztő

2.3 Az adatminősítés elvei

Az információk osztályozását és a rájuk vonatkozó ellenőrzéseket a Középiskola az információ megosztására vagy korlátozására vonatkozó igényekhez, a törvényi előíra-

sokhoz igazítja. Az osztályozás alapján nyilvánvalóvá válik az igény, az elsőbbség és a védettség szintje.

A középiskola informatikai rendszere által kezelt adatok, információk információbiztonsági szempontból a következő kategóriákba sorolhatók:

- Alap védelmi besorolás:
  - ha az adatra nincs kiemelt törvényi szabályozás,
  - az adatvesztés, esetleges nyilvánosságra kerülés kisebb konzekvenciával jár,
  - az alap védelmi besorolású adatok esetében a Középiskola biztosítja, hogy az adat rövid időn belül problémamentesen visszaállítható.
- Fokozott védelmi besorolás:
  - az adatvédelmi előírások hatálya alá tartozó adatok (személyes adatok),
  - törvényben előírt adatszolgáltatással összefüggő adatok,
  - a középiskola feladatainak ellátásához nélkülözhetetlen adatok, kritikus adatok,
  - adatvesztés, megsemmisülés esetén újraelőállításuk hosszadalmas feladat, illetve az adatok integritása ellenőrzésre szorul,
  - azon adatok összessége, amelyekre a középiskola külső személlyel, szervezettel történt megállapodás alapján bizalmas adatkezelési kötelezettség hárul.
- Kiemelt védelmi besorolás:
  - azon adatok, amelyekre titokvédelmi rendelkezés hatálya alá tartoznak,
  - az adatvesztés, esetleges nyilvánosságra kerülés súlyos konzekvenciával jár.

3. A Középiskola fizikai és személyzeti biztonsága

3.1 Környezeti és fizikai biztonság

A Középiskola a nem engedélyezett, illetéktelen hozzáféréseket, behatolást, az ebből következő károkat, rongálást, valamint az adatokkal történő kölcsönhatást megelőzi a fizikai és környezeti védelem megvalósításával.

A Középiskolánál portaszolgálat működik, területére belépési ellenőrzéssel lehet bejutni. Az épületben behatolás jelző rendszer telepített. Az egész épületre kiépített villámvédelem és tűzjelző rendszer van. A villámvédelmet elsődlegesen villámhárító segítségével próbálják megoldani, de villám és túlfeszültség elleni védelemmel ellá-

tott elosztókat is alkalmaznak. Füst- és hőérzékelő található a kiemelt helyeken – biztonsági területeken. Poroltó áll rendelkezésre emeletenként minden lépcsőházi kijáratnál, biztonsági területeken. Az épületben kiépített tűzoltó vízvezeték található, mely veszély esetén azonnal működtethető. A szerverszobában a túlmelegedésre hajlamos berendezéseknél a középiskola a hőmérséklet szabályozására klimatizációról gondoskodik.

A Középiskola, ahol szükséges, biztonsági területeket különít el és alkalmaz, a kiemelt védelmet igénylő információ-feldolgozó eszközöket tartalmazó területek, a speciális biztonsági követelményekkel rendelkező szobák és eszközök védelme érdekében. Biztonsági terület a szerverszoba és az informatikai tanárok helységei, mely kulcsra zárhatók, belépés csak az arra feljogosítottak számára lehetséges.

A biztonsági területeken harmadik fél által történő munkavégzés minden esetben megfelelő felügyelet és ellenőrzés biztosítása mellett végezhető. Az ellenőrzés, a jogosultságok meghatározása és engedélyezés az munkahelyi vezető, a megvalósítás az illetékes rendszergazda feladata.

A Középiskola a berendezések védelme érdekében:

- beléptető rendszerrel, behatolás- és tűzjelzés-riasztással, épületbe léptetési renddel, épület-felügyelettel biztosítja az általános védelmet,
- a berendezések elhelyezésével, a jelszóvédelem szabályozott alkalmazásával biztosítja a jogosulatlan hozzáférés lehetőségének minimalizálását a veszélyeztetett területeken,
- a berendezések áramellátását szünetmentes tápegységekkel és megfelelően méretezett részhálózatokkal biztosítja,
- irodatechnikai, informatikai eszközei karbantartását és javítását többnyire saját embereivel, illetve alvállalkozóval végezteti, a rendellenességeket naplózzák,
- a középiskola szabályozza a mobil eszközök használatát,
- a berendezések értékesítésekor a tárolt adatok törlését elvégzi a szabályozás szerint.

3.2 Személyzeti biztonság

A középiskola informatikai biztonsági elveivel összhangban kiemelt figyelmet fordít alkalmazottainak, alvállalkozóinak kiválasztására, kezelésére és ellenőrzésére, hogy megelőzze az emberi hibákat és visszaéléseket.

A közalkalmazotti munkakörben a munkavállalók titoktartását törvényi szabályozás biztosítja, egyéb munkavállalók esetében a munkavállalók titokvédelmi nyilatkozatot írnak alá. A harmadik félnek – szükség szerint – külön titoktartási megállapodást kell aláírnia, még mielőtt az információ-feldolgozó eszközökhöz hozzáférést nyerne.

4. A Középiskola informatikai eszközrendszere

A középiskola tulajdonában lévő számítástechnikai eszközök az alábbi csoportokra oszthatók:

a) számítógépek (szerverek, munkaállomások, hordozható számítógépek, egyéb számítógépek)

b) nyomtatók és multifunkcionális eszközök

c) adatrögzítők és tárolók

d) szünetmentes tápegységek

e) szkennerek

f) faxok

g) multifunkcionális fénymásoló

A részletes leírásokat az aktuális hardver-szoftver nyilvántartás tartalmazza.

4.1 Nyilvántartások

A Középiskola hardvereszközeiről nyilvántartást vezet. A nyilvántartás tartalmazza: az eszközök konfigurációját, az alkalmazó szervezeti egységet, az eszközökre jellemző fontosabb adatokat.

A Középiskola alkalmazott szoftvereiről nyilvántartást vezet. A nyilvántartás tartalmazza: az alkalmazott szoftver megnevezését, számát, a felhasználás helyét.

4.2 Az informatikai hálózat

A Középiskola informatikai rendszerének logikai hálózati ábráját a Szabályzat 12 sz. pontjában található melléklet tartalmazza.

5. Az informatikával kapcsolatos feladatkörök

A Táncsics Mihály Szakközépiskola, Szakiskola és Kollégiumnál a betöltött munkakörtől függően szükséges a számítógép, a felhasználói alapszoftverek (szövegszerkesztő, táblázatkezelő stb.), kiegészítő szoftverek (jogszabály stb.) és a Középiskola különböző területein fejlesztett vagy használt célszoftverek (pl. könyvelés, tanulónyilvántartás) ismerete és biztonságos kezelése.

Az egyes munkaköröket betöltő munkatársaknak a 10.1 mellékletben részletezett informatikai ismeretekkel kell rendelkeznie.

6. A Középiskola informatikai eszköz használatának szabályai

6.1 Általános szabályok

Az informatikai rendszer célja a felhasználók azon igényeinek kielégítése, amelyek az iskola Pedagógiai Programjában és a Szervezeti és Működési Szabályzatában megfogalmazott oktatási tevékenységekkel kapcsolatosak, ezért az informatikai rendszer csak ezen célok elérésére használható, az iskola szándékainak megfelelően.

Ennek megfelelően az informatikai rendszer erőforrásait külön engedély nélkül tilos kereskedelmi, vagy egyéb nem iskolai célra használni. Megengedett az informatikai rendszer magáncélra (pl. magánjellegű levelezésre) történő felhasználása, ha ez nem jelent indokolatlanul nagy terhelést a rendszernek, veszélyeztetve ezzel az oktatási-nevelési célok megvalósítását.

6.2 A Középiskola munkatársainak kötelezettségei

Az informatikai eszközrendszerek használata során a Középiskola valamennyi munkatársa köteles

- a munkaállomását a jogosulatlan használattal szemben biztonságossá tenni jelszavas védelem alkalmazásával,

- a megfelelő gondossággal eljárni. Ez egyrészt azt jelenti, hogy mindenki köteles a rendelkezésére bocsátott eszközöket (számítógépek és perifériák) tisztán tartani, minden káros hatástól óvni, a munka végeztével a gépeket kikapcsolni;
- az általa használt számítógép "belső tisztaságára" is ügyelni, a felesleges fájlokat kitörölni,
- a megfelelő be- és kilépési eljárásokat végrehajtani,

Tilos a Középiskola számítástechnikai eszközeit az iskolán kívül használni, kivéve, ha erre külön írásbeli utasítást kap valaki, valamint kivéve a hordozható eszközöket (pl. notebookok).

Ezek használata mindig feljogosított személyhez kötött. A hordozható eszközök használatára külön fejezetben leírt szabályok érvényesek.

6.3 A tanulók kötelezettségei

Mivel a tanórák alatt a tanulók is az informatikai rendszer felhasználóivá válnak, így nekik is kötelességük betartani a szabályzatot. Alapvető szempont az informatikai rendszer órák alatti használatánál, hogy a tanulók csak a tanár utasításait követve dolgozhatnak, mind a gépek tényleges használata során, mind pedig a kiadott feladatok megoldása, vagy tananyag feldolgozása közben. A következőkben megtalálható néhány fontos szabály, amik betartása minden tanulóra nézve kötelező:

- A géptermekben tanár felügyelete nélkül tartózkodni tilos.
- A gépeket bekapcsolni csak a tanár kifejezett utasítására lehet.
- A termekben található elektromos csatlakozásokhoz, vezetékekhez, a gép kábeleihez nyúlni, a gépek burkolatát kinyitni, eltávolítani tilos.
- A tanárok és más iskolai dolgozók által használt gépeket (tanári szoba, titkárság, igazgatói szoba, gazdasági iroda, szaktanári szobák gépeit) tanuló nem használhatja.
- A gépterembe ételt, italt, bármilyen élelmiszert fogyasztani tilos.
- A tanórák alatt történő bármilyen rendellenes működést, sérülést, rongálást azonnal jelenteni kell a tanárnak.

6.4 Az informatikai rendszerhasználat korlátozásai

Az informatikai rendszer nem használható az alábbi tevékenységekre:

- az érvényes magyar jogszabályokba ütköző cselekmények, ideértve a következőket, de nem korlátozódva ezekre: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftverek szándékos és tudatos illegális használata, terjesztése;
- az informatikai rendszerhez kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik;
- haszonszerzést célzó, közvetlen üzleti célú tevékenység, reklámok terjesztése;
- az informatikai rendszer, illetve erőforrásai szabályos működését megzavaró, veszélyeztető tevékenység;
- az informatikai rendszert, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, SPAM);
- az informatikai rendszer erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata (például mások leveleinek elolvasása hagyományosan jogszabályba ütköző tevékenység, és ez az elektronikus levelekre is vonatkozik, tehát ez a levéltitok megsértésének minősül);
- az informatikai rendszer erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére irányuló bármilyen tevékenység;
- az informatikai rendszer biztonságát veszélyeztető információk, programok használata, terjesztése, tárolása;
- vallási, etnikai, politikai, erkölcsi vagy más jellegű érzékenységet sértő, másokra nézve sértő, esetleg másokat zaklató tevékenység (pl. szélsőséges nézeteket képviselő, fajgyűlölő, vagy pornográf anyagok megtekintése, tárolása, közzététele vagy továbbítása);
- mások munkájának indokolatlan és túlzott mértékű zavarása, vagy akadályozása (pl. kéretlen, zaklató levelek küldése);
- a hálózati erőforrások magáncélra való túlzott mértékű használata.

Lényeges kitérni arra, hogy a szellemi alkotásokat hagyományosan szerzői jogok védik. Erre a védelemre nevének megadásával automatikusan jogosult a szerző. A szerzői jogok védelmére nemzetközi egyezmények vonatkoznak, melyek Magyarországon

is érvényesek, tehát az iskola nem nézheti el ezek megsértését. "Copyright" által védett szoftvert csak az idevonatkozó szerződéssel összhangban lehet használni. A szerzői jogok megsértése bűncselekmény.

Kiemelten tiltott tevékenységek

- Bejelentkezési kísérletek

Tilosak a bejelentkezési kísérletek olyan gépre, melyre az igénybevevőnek nincs jogosultsága. Tilos más ismert, nem saját felhasználói néven történő bejelentkezési kísérlet, vagy a "névtelen" felhasználói nevek használata kifejezett engedély nélkül. Határozottan tiltott dolog a SUPERVISOR, ADMINISTRATOR illetve más kiemelt jogosultsággal rendelkező felhasználói néven való próbálkozás, illetve a jelszó megszerzésére tett kísérlet.

- Betörési kísérletek, biztonsági rendszabályok megsértése

- Tilos az informatikai rendszer biztonsági rendszerében levő hibák, hiányosságok kihasználásával privilégiumok (előnyök) szerzése. Amennyiben a sikeres betörést a felhasználó a rendszergazda tudtára hozza, mielőtt az észlelné, és semmilyen károkozás nem történt, "felmentésben" részesül, hiszen hozzájárult az informatikai rendszer biztonságának növeléséhez.
- Más felhasználói nevének használata még annak engedélyével is tilos!
- A felhasználói név kölcsönadása (átruházása) még ideiglenesen is tilos!
- Másvalaki jelszavának kiderítésére irányuló bármely kísérlet tilos!
- Bármely adatállomány átvitele más adattárolóra, más gépre vagy a hálózatra az állomány tulajdonosának tudomása, vagy szándéka nélkül tilos!

Különösen elfogadhatatlan, ha a bejelentkezési/betörési kísérletek iskolán kívüli, illetve külföldi gépre történnek. Ennek ugyanis következménye lehet az iskola, mint intézmény felelősségre vonása, esetleg az iskola, vagy a teljes Sulinet hálózat kizárása egyes rendszerekből.

A számítógép vagy szoftvereinek másokat sértő használata számítógépes zaklatás! (A címzettet felháborító, esetleg fenyegető levelek, képek, üzenetek küldése, mások munkájának akadályozása tilos!)

- Számítógépes játékok

Az iskola nem támogatja a számítógépes játékok iskolai gépek adattárolóira való másolását, tárolását. Ez alól a szabály alól kivételt képeznek azok a fejlesztő jellegű játékok, oktatásai anyagok, melyeket az iskola megvásárolt, vagy használatukra engedélyt kapott, és az Üzemeltetés a munkaállomásokon vagy a hálózaton kimondottan e célra elhelyezett.

- Tilos továbbá

- erőforrás használata olyan módon, hogy erről az Üzemeltetésnek nincs tudomása;
- erőforrás pazarlása másokat akadályozó, vagy az informatikai rendszer biztonságos működését veszélyeztető mértékben;
- a jogosított személyek akadályozása jogos tevékenységükben;
- számítógépek vagy bármely, az informatikai rendszerhez tartozó berendezés engedély nélküli megbontása, ki- vagy bekapcsolása, beállításainak megváltoztatása;
- bármilyen szoftver-beállítás engedély nélküli megváltoztatása.

7. Számítástechnikai eszközök beszerzése, nyilvántartása, használatból történő kivonása

Beszerzés

Az eszközbeszerzéssel kapcsolatos eljárásoknál a vonatkozó jogszabályok, illetve minőségügyi eljárások szerint kell eljárni. Informatikai eszközök beszerzését általános igazgatóhelyettes koordinálja. Az igazgatóhelyettes az informatikai költségvetésére vonatkozó javaslatot minden év október végéig elkészíti és leadja.

A Középiskola — az informatikai politikájában foglaltaknak megfelelően — minden munkatársa számára biztosítja az illető munkájához szükséges és elégséges szoftverellátást. A szükséges és elégséges mértéket a személyi használatra üzembe helyezett számítógépeken az azon dolgozó munkatárs feladataiból, a folyamatosan több munkatárs által használt számítógépeknél pedig a számítógép funkciójából kerül meghatározásra. A felhasználói igényeket az általános igazgatóhelyettes gyűjti össze és körültekintően intézkedik az igény kielégítéséről.

Informatikai eszközök és szoftverek beszerzésére a Középiskola éves költségvetési tervének megfelelően, központilag kerülhet sor. A beszerzésre kerülő eszközökről az iskolavezetés dönt.

Üzembe helyezés (használatbavétel)

Az eszközöket a tervezett felhasználás alapján adják ki az igénylő szervezeti egységnek. Az átadás-átvétel és az eszköz üzembe helyezés a rendszergazda feladata.

Hardver nyilvántartás

Beérkezéskor az eszközök mennyiségi, kiadáskor a minőségi átvételét kell elvégezni. Az átvételkor az eszközt a leltári szabályoknak megfelelően el kell látni leltári számmal, és egyidejűleg a leltár és az informatikai nyilvántartásba is fel kell venni. Az informatikai nyilvántartásnak meg kell egyeznie a leltári nyilvántartással.

Szoftver nyilvántartás

A rendszergazda az eredeti programot a licensz engedéllyel együtt biztonságos helyen tárolja, és egyidejűleg vezeti e Szabályzatban meghatározott nyilvántartást. A szoftver kézikönyvét, a felhasználók által hozzáférhető helyen kell tárolni.

Ezen túlmenően számítástechnikai szakmai és információbiztonsági, valamint szoftver jogtisztasági szempontok miatt az alábbi szabályokat is be kell tartani:

- A Középiskolánál üzembe állított számítógépekről nyilvántartást kell vezetni.
- A nyilvántartást munkahelyenként (gépenként) és összesítve is ki kell dolgozni.
- A nyilvántartásnak feltétlenül tartalmaznia kell a következő adatokat:
  - A hálózatban üzemelő gép helyét,
  - a gépért felelős személy adatait,
  - a gép pontos konfigurációját (processzor típusa, memória mérete, diszk mérete stb.), leltári azonosítóját, a beszerzés idejét
  - a gépen futó szoftvereket (verzió szerint).

8. A Középiskola informatikai rendszerének üzemeltetési szabályai

Az SZMSZ szerint az informatikai ügyekért az általános igazgatóhelyettes felel. Informatikai jellegű munkáját a három részmunkaidőben alkalmazott rendszergazda segíti. A fejlesztés alapvetően szakképzési pénzekből történik, így az informatikai munkaközösség vezetőnek szorosan kell együttműködni azokkal a kollégákkal, akik a szakképzési pénzekkel foglalkoznak (gyakorlati oktatásvezető).

A Középiskola informatikai rendszere üzemeltetésének szabályozása során két alapterülettel kell foglalkozni, ezek definíciószerűen a következők:

- *információvédelem*, amely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni.
- *az informatikai rendszer megbízható működése:* amely az adatok rendelkezésre állását és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitását hivatott biztosítani

Az alábbi szabályozások e két alapterülettel foglalkoznak, és a következő területeket érintik:

1. Az informatikai rendszer üzemeltetését biztosító személyzet
2. Az informatikai rendszer egészét érintő általános intézkedések
3. Rendszerelemekhez kapcsolódó intézkedések
4. Az adatfeldolgozás folyamatához kapcsolódó intézkedések
5. A Katasztrófaterv

8.1 A Középiskola informatikai rendszerének üzemeltetését biztosító személyzet

- A rendszeradminisztrátori, illetve a fontosabb alkalmazások rendszergazdai funkcióját lehetőleg személyükben szét kell választani.
- Munkába álláskor minden informatikai munkatárs számára biztosítani kell az informatikai biztonsággal kapcsolatos, feladatköre ellátásához szükséges ismeretek, feladatok elsajátítását. Az elsajátítás tényét, valamint azt, hogy a Középiskola Informatikai Szabályzatában foglaltakat magára nézve kötelezőnek tartja, minden munkatársnak aláírásával igazolnia kell. A nyilatkozat mintát a melléklet 10.2 pontja tartalmazza

- Az informatikai rendszer biztonságos működésének fenntartása érdekében a megfelelő szintű továbbképzésről rendelkezni kell a Középiskola éves képzési tervében;
- Az informatikai munkatársak új munkakörbe történő átsorolása, áthelyezése esetén, továbbá új alkalmazások, technológia bevezetésénél ugyancsak biztosítani kell a megfelelő szintű képzést, továbbképzést.
- Az informatikai rendszer biztonságát meghatározó munkakörökben dolgozó munkatársak kiválasztásánál a biztonság szempontjait fokozottan figyelembe kell venni. Gondoskodni kell arról, hogy az ideiglenesen vagy tartósan távollévő munkatárs feladatát arra alkalmas, megfelelően felkészített helyettes vegye át.
- Külső partnerekkel kötött fejlesztési, karbantartási szerződés részeként, az Informatikai munkaközösség vezetővel történt egyeztetés után, a külső partner számára kötelező érvénnyel elő kell írni a Középiskola Informatikai Szabályzatának rájuk vonatkozó szabályait, amelyek megsértése jogi és kártérítési eljárást von maga után.

A belépő munkatársakkal kapcsolatos informatikai vonatkozású intézkedések:

- a Középiskolával fő- vagy részmunkaidőben közalkalmazotti jogviszonyt vagy munkavállalói viszonyt létesítő munkatársakkal ismertetni kell az informatikai szabályzatból rá vonatkozó szabályokat és szabályozásokat,
- a különböző adatbázisokat előállító, illetve azokkal dolgozó munkatársak személyes nyilatkozatban rögzítik, hogy az adatok kezelésére, tárolására, forgalmazására, továbbadására, értékesítésére vonatkozóan mindenkor betartják az érvényes külső és belső szabályzatokat, utasításokat, szerződéseket,
- ellenőrizni kell, hogy a betöltendő munkaköréhez kapcsolódó számítástechnikai szakmai képzettséggel rendelkezik-e, amennyiben szükséges, a megfelelő intézkedéseket kezdeményezni kell (beiskolázás, stb.),
- az új munkatársak számára létre kell hozni az informatikai eszközök alkalmazásához szükséges hálózati környezetet (e-mail fiók, hálózati könyvtár, jogosultsági beállítások, stb.),
- a belépő munkatársnak nyilatkozatot kell tenni a szoftverhasználati politika tudomásul vételéről és betartásáról. (melléklet)

A kilépő munkatársakkal kapcsolatos informatikai vonatkozású intézkedések:

- kilépő munkatársakról az Informatikai munkaközösség vezető értesítést kap a terület vezetőjétől,
- szükség esetén időszakos titoktartási nyilatkozatot kell kötni,
- biztosítani kell a munkaeszköz átvételét, különös tekintettel a személyes használatú munkaállomásokon tárolt adatokra,
- biztosítani kell a levelezés archiválását, átirányítását, illetve megszüntetését,
- a hálózati környezet letiltását.

A tanulókkal kapcsolatos informatikai vonatkozású intézkedések:

- a tanulóval ismertetni kell az informatikai szabályzatból rá vonatkozó szabályokat és szabályozásokat,
- az új tanulók számára létre kell hozni az informatikai eszközök alkalmazásához szükséges hálózati környezetet (e-mail fiók, hálózati könyvtár, jogosultsági beállítások, stb.),
- végzett tanulók esetén biztosítani kell a levelezés archiválását, átirányítását, illetve megszüntetését, illetve a hálózati környezet letiltását.

8.2 Az informatikai rendszer egészét érintő általános intézkedések

8.2.1 Hozzáférés jogok szabályozása

A hozzáférési jogosultságok megfelelő szabályozásával, a jelszó azonosítási rendszerrel a Középiskola biztosítja, hogy a felhasználók csak azokhoz a szolgáltatásokhoz férhetnek hozzá közvetlenül, amelyek használatára kifejezetten fel vannak hatalmazva.

Az információvédelmet biztosító informatikai rendszerben:

- A rendszer felhasználóihoz hozzáférési jogokat kell rendelni. A jogokat minimálisan egyedi, illetve csoport tulajdonosi szinten kell tudni megadni. Az egyértelmű jogosultság szabályozás kialakítása céljából célszerű a felhasználók és a rendszer által nyújtott szolgáltatások biztonsági követelmény-mátrixát felállítani.
- A hozzáférés jogosultság menedzselésénél a szabad belátás szerint kialakított *hozzáférés-vezérlés* elvét kell alkalmazni a következő hozzáférési jogokkal:

  - olvasási jog (betekintés),
  - írási jog (létrehozás, módosítás),
  - törlési jog.
- A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoport szinten történő megkülönböztetésére és szabályozására.
- A rendszer objektumaihoz (fájlok, eszközök, processzek közötti kommunikációs csatornák) egyedi, illetve csoport tulajdonosokat kell rendelni az objektum létesítésekor. A hozzáférés vezérlése esetén az adott objektumhoz (pl. fájl) esetenként (pl. létesítéskor) rendelődnek hozzá a tulajdonosok jogai is.
- A hozzáférési események esetén jogosultság ellenőrzést kell végrehajtani. A hozzáférés-vezérlés a szubjektumokhoz (felhasználók, processzek) rendelt jogok és az objektumokhoz rendelt tulajdonosok és jogaik összevetése alapján történik.
- A jogosultsági rendszernek támogatnia kell a jogosultságok módosítását, átadását másik személynek, törlését és időleges korlátozását. Új jogosultság kiosztását, a jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott rendszeradminisztrátor végezheti el.
- A jogosulatlan hozzáférési kísérleteket rögzíteni kell a biztonsági naplóban, amelynek értékelését rendszeresen el kell végezni.
- On-line adatmozgás (tranzakció) kezdeményezésének jogosultságát minden esetben ellenőrizni kell.
- A rendszeradminisztrátorok jogosultsági rendszerének kialakításakor speciális figyelmet kell fordítani a rendszer-parancsok és adatállományok használatának szigorú és egyértelműen körülhatárolt szabályozására.

A hozzáférési jogosultságok meghatározása és kiosztása a Középiskola ezen Szabályzatának megfelelő módon történik, a hozzáférési jogosultságok meghatározása az adott terület vezetőjének írásos javaslata alapján az Informatikai munkaközösség vezető feladata. A felhasználó hozzáférési jogainak belépéskor illetve új munkakörbe helyezésekor az adott terület vezetőjének írásban történő engedélyezése alapján valósítható meg (10.3 melléklet).

Alapértelmezésben a diákok a központi számítógépen 50 MB tárhellyel rendelkeznek, míg a tanárok számára 250 MB áll rendelkezésre.

8.2.2 Azonosítási és hitelesítési rendszer

A Középiskola informatikai rendszerének üzemszerű, folytonos és biztonságos használata érdekében az azonosítási rendszer a következők szerint kerül kialakításra:

- a rendszer egészére minden alany (felhasználók és programok) számára logikailag egyetlen azonosító használatát kell biztosítani (egy felhasználó – egy azonosító);

Az informatikai rendszer használata során a felhasználók kötelesek a jelszavas védelmet alkalmazni. Az egyedi felhasználókat és a felhasználó csoportokat jelszóval kell azonosítani. A jelszavak megválasztásakor az általánosságban elfogadott biztonsági előírásokat be kell tartani. Jelszóképzésnél a négy alaptípusból (kisbetű, nagybetű, számjegy, írásjel) legalább három félét kell alkalmazni.

A jelszó hossza

- Felhasználói jelszavak esetén legalább 6 karakter
- Rendszergazdai jelszavak esetén legalább 8 karakter kell legyen.

A jelszó kiválasztásakor figyelemmel kell lenni arra, hogy a jelszó az alkalmazó személyes körülményeivel, adataival ne legyen összefüggésbe hozható. Rendszerbeállítással (felhasználó kezelés) elő kell írni a jelszavak 90 naponkénti folyamatos változtatását. Ennek szabályai a következők: Kisbetű, nagybetű, szám, különleges karakter, ebből a négy típusból legalább háromnak lennie kell és a jelszavak öt alkalomig nem ismétlődhetnek.

- Minden felhasználó felel a rábízott felhasználói azonosító és az ahhoz rendelt jogok biztonságáért. Az azonosító használatra másnak még a tulajdonos jelenlétében sem engedhető át.
- A felhasználói azonosítóhoz tartozó jelszót csak annak birtokosa ismerheti.
- Amennyiben felmerül a gyanú, hogy a jelszó mások tudomására jutott, úgy azt azonnal meg kell változtatni.
- Amennyiben valaki észleli, hogy mások kísérletet tesznek a felhasználói jelszavak megszerzésére, azt azonnal jelezni kell a rendszergazdának.
- Minden, más személy jelszavának vagy adatainak megszerzésére irányuló cselekedet súlyos fegyelmi vétség.
- A felhasználói azonosító tulajdonosa elsődlegesen felel az azonosító használatával elkövetett szabálytalanságokért. Akkor is felelősségre vonható,

hogyha bebizonyosodik, hogy azt nem ő használta, de gondatlansága folytán jutott az azonosító illetéktelen kezekbe.

- Ennek érdekében a felhasználó a számítógépes munkahely elhagyásakor minden alkalommal köteles kilépni a hálózatból.
- A felhasználói jelszó átadását senki sem kérheti.

A rendszeradminisztrátori jelszavakat (gépek illetve szerverek) vészhelyzet esetére páncélszekrényében, lezárt, lepecsételt borítékban kell tartani. Kinyitására az igazgató adhat engedélyt. A felnyitás okát és tényét jegyzőkönyvben kell rögzíteni.

Adott számú téves bejelentkezési kísérlet után az adott felhasználói jogosultsági rendszert bénítani kell, a téves bejelentkezés ténye rögzítendő és kivizsgálandó.

Ahol indokolt, ki kell alakítani a többszintű (pl. operációs rendszer, adatbázis-kezelő, levelező rendszer, irodaautomatizálási rendszer stb.) hitelesítési és azonosítási rendszert az egyes szoftverek által nyújtott biztonsági funkciók, az alkalmazási területek és a biztonsági követelmények figyelembevételével.

8.2.3 Auditálás

Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert (biztonsági napló) kell kialakítani, hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint illetéktelen hozzáférés megtörténtét.

8.2.4 Vírusvédelem

Biztosítani kell a Középiskola egészére kiterjedő, rendszeres és folyamatos vírusvédelmet kereskedelemben kapható, kiterjedt referenciával rendelkező szoftverekkel.

A rendszerbe kívülről bekerülő adathordozókat felhasználás előtt vírusellenőrzésnek kell alávetni. Az alkalmazásszintű védelem használatánál ugyanakkor biztosítani kell, hogy ne gyengítse az operációs rendszer szintjén megvalósított, vagy megvalósítható védelmet.

A felhasználói munkaállomások vírusvédelme

A Középiskola hálózatán kívüli területről (floppy lemez, CD, Internet, elektronikus levél, stb.) érkező adatokat – az adathordozó jellegétől függetlenül – felhasználásuk előtt alá kell vetni a Középiskola hálózatán használatos vírusvédelmi programmal való ellenőrzésnek.

A külön modemes kapcsolattal rendelkező önálló munkaállomás a hálózati üzem szempontjából Középiskolán kívüli területként kezelendő. Aki az adatállományait és adathordozóit a vírus ellenőrzés vagy vírusvédelmi intézkedés (vírus vizsgálat és irtás) alól bármilyen indokkal kivonja, az abból eredő károkért felel.

Játékprogram vagy nem szervezeti (oktatási) célú programállomány még vírus ellenőrzés esetén sem tölthető be, nem tárolható és nem futtatható. Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás nem üzemeltethető.

A munkaállomásokon állandó figyelést (víruspajzs) biztosító vírusvédelmet kell használni. Vírusvédelmi programot a felhasználó által ki nem kapcsolható, felhasználói beavatkozástól független frissítési opcióval kell telepíteni.

Heti 1 alkalommal a teljes merevlemezt automatikusan le kell ellenőrizni. A program futásakor észlelt rendellenességet vagy vírust azonnal jelezni kell a rendszergazdának. A rendszergazda által központilag indított egyedi vírusvizsgálatot, a munkaállomást használó felhasználó nem tilthatja le.

A vírusvédelem rendszerüzemeltetési szabályai

Telepített vírusvédelmi program nélkül a Középiskola területén munkaállomás nem üzemeltethető.

A vírusvédelmi szoftver legfrissebb változatának az Interneten keresztül való letöltéséért, a Középiskola szerverein és munkaállomásain való frissítéséért és működéséért és a hálózat vírusmentes állapotának ellenőrzéséért a kijelölt rendszeradminisztrátor felelős.

A felhasználói munkaállomásokon le kell tiltani a floppy lemezről és CD-ről való rendszerbetöltés és indítás (bootolás) lehetőségét. Floppy meghajtó vagy CD használatát csak a munkavégzés által indokolt feladatkörben szabad támogatni.

Konkrét vírus detektálásáról a felhasználó munkaállomásának azonosító adataival (dátum, felhasználó neve, leltári szám, munkaállomás azonosító) és a vírusdetektáló program által rögzített vírus információs „riport” adataival ellátott jelentést kell készí-

teni az Informatikai munkaközösség vezető részére, aki dönt a szükséges óvóintézkedések kiadásáról.

Ha a vírustámadás behatolási pontja nem lokalizálható illetve a veszély működés közben nem elhárítható, az Informatikai munkaközösség vezető a hálózat egyes funkcióit, vagy a teljes hálózat szolgáltatásait jogosult egy napra felfüggeszteni.

8.2.5 Karbantartás és javítás

A hardver elemeknél a megelőző karbantartást az adott elemre vonatkozó karbantartási előírásoknak megfelelő gyakorisággal és szakmai szinten kell elvégezni. Hardver elemek műszaki felülvizsgálatát a rendszergazdák végzik évente egyszer időszakonként.

A szervezet olyan informatikai beszerzési és fenntartási stratégiát alakítson ki, amelynek keretében:

- A szállítóval és a szerviz cégekkel olyan garanciális, illetve garancián túli szerviz szerződést kell kötni, amely garantálja az alapbiztonsági osztályra meghatározott *rendelkezésre állás*i szint betarthatóságát.
- A hardver rendszerre a szállítónak minimum 1 éves garanciát kell vállalnia. A rendszer értékétől függően 5-10 évig kell biztosítania a tartalék alkatrészellátást.
- Biztosítani kell a rendszer felfelé való kompatibilitását mind hardver, mind szoftver szempontból úgy, hogy a rendszer bővíthetősége, az alkalmazói rendszerek hordozhatósága hosszú távon biztosítható legyen.

A berendezések házon kívüli karbantartásakor az információvédelmi alapelveket figyelembe kell venni.

8.2.6 Informatikai biztonsági ellenőrzés

Az informatikai biztonsági ellenőrzések alapvető célja, hogy a kockázatok csökkentése és a rendkívüli események elkerülése érdekében objektív információkat szolgáltasson a felelős vezetők számára az informatikai biztonság helyzetéről.

A megállapításokat mindig írásos jelentésbe kell foglalni, a védelmi intézkedések megsértésével kapcsolatban adott esetben szankciókat is kell alkalmazni.

8.3 Rendszerelemekhez kapcsolódó intézkedések

8.3.1 Adathordozók

Az adatátvitelre, mentésre, valamint archiválásra használt adathordozókat az alapbiztonságban érvényes tűz- és vagyonvédelmi előírásoknak megfelelően védett, zárt helyiségben kell tárolni.

A tároló helyiségben az adathordozók minőségi jellemzői megtartása céljából a környezeti feltételeket (hőmérséklet, pára- és portartalom) biztosítani és ellenőrizni kell.

Az adathordozókra érvényes általános szabályozások a következők:

- az adathordozók beszerzésére, az azokkal való gazdálkodásra, készlet- és használat nyilvántartásra, valamint készlet feltöltésre az általános beszerzési szabályok vonatkoznak,
- a Középiskolánál a mentésre, archiválásra szolgáló adathordozók tartalmát nyilván kel tartani,
- az adathordozókat használatba venni csak az előírt ellenőrző eljárások (pl. vírusellenőrzés) után szabad,
- ki kell alakítani az adathordozók másodpéldányai (biztonsági másolatok) biztonságos tárolásának feltételeit (tűzbiztos páncélszekrény vagy elkülönített tárolás),
- ki kell alakítani a rendszer- és felhasználói szoftver törzspéldányok biztonságos tárolásának feltételeit (tűzbiztos páncélszekrény vagy elkülönített tárolás),
- megelőző intézkedésekkel - meghatározott időszakonkénti ellenőrzéssel - meg kell akadályozni az elöregedésből fakadó adatvesztést.

8.3.2 A hardvereszközök biztonsági védelmi eljárásai

A számítástechnikai eszközök esetében a felnyitás elleni védelemről a ház kulccsal történő zárásával vagy a rögzítő csavarok plombálásával, pecsételésével kell gondoskodni.

Azoknál a személyi számítógépeknél, amelyeknél a floppy vagy CD író egység használata nem indokolt és azt a logikai védelem eszközeivel letiltani nem lehet, a beépítésre nem kerülhet sor, vagy utólag el kell távolítani, illetve megfelelő eszköz alkalmazásával le kell zárni.

Bármely típusú munkaállomásnál ki kell alakítani a felhasználók különböző szintjeinek megfelelő belépési lehetőséget. Ilyen felhasználói szintek lehetnek például:

- egyedi felhasználós munkahely,
- több felhasználós munkahely,
- rendszergazda munkahely,
- adminisztrátori munkahely.

A munkaállomásoknál gondoskodni kell arról, hogy a felhasználó hosszabb inaktivitása után kényszerített kijelentkezéssel vagy az alapegységek használhatóságának korlátozásával (pl. a billentyűzet blokkolásával, a képernyő elsötétítésével) az illetéktelen használat meg legyen akadályozva.

A fejlesztői és a normál felhasználói munkahelyeket egymástól szigorúan el kell különíteni.

8.3.3 Szoftverek biztonságos üzemeltetésének általános kérdései

A beszerzendő szoftver termékeket bevezetés előtt be kell vizsgálni a sértetlenség, a funkcionalitás teljesülése és a stabil működés szempontjából. Beszerezni, illetve installálni csak jogtiszta, megfelelő dokumentációval ellátott, vírus és hibamentességre tesztelt szoftvert szabad.

Az általános igazgatóhelyettes és/vagy rendszergazda engedélye nélkül idegen vagy a szervezethez nem tartozó munkatársak által fejlesztett szoftver nem installálható.

Hálózati alapú rendszereknél törekedni kell egy kiválasztott szerverre alapozott központi szoftver-menedzsment (installáció, változat-követés, megszüntetés) kialakítására. Szoftver installációt csak az erre felhatalmazott rendszeradminisztrátor(ok) végezhet(nek) el a teljes informatikai rendszerben.

A szállítónak legalább 3 éves távon biztosítania kell a nagy értékű szoftverrel kapcsolatos szavatosságot és támogatást. Ha a szállító részéről megszűnik a szoftvertámogatás, a felhasználónak a forráskód birtokába kell jutnia, hogy a támogatást akár saját erővel, akár külső kapacitással biztosítani tudja.

Az újonnan beszerzett szoftvereket nyilvántartásba kell venni, az installáció módját és feltételeit az informatikai rendszer ismeretében konkrétan kell kialakítani. Új szoftver

installálása előtt az érintett alrendszer (szerver[ek]) vagy munkaállomás) adatait menteni kell.

8.3.4 Dokumentáció, dokumentumok

Az informatikai rendszer biztonságát érintő adatokat tartalmazó dokumentációhoz csak az arra felhatalmazott személyek férhetnek hozzá.

Az informatikai rendszer vagy annak bármely eleme csak az arra illetékes személy felhatalmazásával, dokumentáltan változtatható meg, amelyet ellenőrizni kell.

8.3.5 Elektronikus üzenetkezelés, elektronikus levelezés és ellenőrzése

Biztosítani kell, hogy az elektronikus úton továbbított üzenetek, állományok tekintetében az iratkezelési szabályzatban meghatározott, a papíralapú dokumentumokra vonatkozó — az elektronikus adatátvitel sajátosságainak megfelelő — eljárási rend érvényesüljön. Ennek érdekében levélküldés, fájl átadás esetében biztosítani kell az előírás szerinti iktatás (pl. átvitel naplózása és üzenetek archiválása) feltételeit.

A Középiskola a kapcsolattartás folyamatában kiemelt szerepet szán az elektronikus levelezésnek és az elektronikus csoportmunka kezelésnek.

- Az adatvédelem és adatbiztonság érdekében olyan csoportmunka üzenetkezelő és elektronikus levelező rendszert kell alkalmazni, mely az üzeneteket kódolt illetve nem szövegállomány formátumban tárolja.
- A Középiskola külvilág felé irányuló üzenetforgalmát tartalmi betekintés nélkül a rendszer naplózza.
- Gondoskodni kell a vírusvédelemnek a levelező szolgáltatásokra történő kiterjesztéséről, ezen keresztül a központi vírusadatbázis letöltéséről, és a munkaállomások közötti automatikus szétosztásáról.

8.3.6 A hordozható számítógépes eszközök használatának szabályai

Az eszközök kezelése

A hordozható számítógépes eszközök közül külön szabályozás alá a notebookok (laptopok) és mobil adattárolók (merevlemezek) tartoznak. Minden mobil eszközről önálló üzemeltetési naplót kell vezetni.

Az üzemeltetési naplóban

- rögzíteni kell az eszköz valamennyi fő jellemzőjét (gyártó, sorozatszám, konfiguráció, engedélyezett felhasználási területek, installált programok, az eszközön tárolt adatok),
- valamint folyamatosan vezetni kell a felhasználásra vonatkozó adatokat (felhasználó személy, a felhasználás célja és ideje)

A mobil eszközök használata során, amennyiben azok a Középiskola működését érintő lényeges adatokkal kerülnek felhasználásra különös hangsúlyt kell fektetni az eszközön ideiglenesen tárolt adatok védelmére.

Adatvédelem, mobil eszközökön

A hordozható számítógépes eszközök külső felhasználása során különös gondot kell fordítani az eszközök fizikai és adatvédelmére. A védelemért mindenkor az üzemeltetési naplónak megfelelő felhasználó felelős.

Általános védelmi szabályok:

- Notebook esetében az eszközök jelszavas védelmét alkalmazni kell a bekapcsolásra és a BIOS-hoz történő hozzáférésre.
- A hordozható számítógépek csak a Középiskola adatvédelmi előírásait kielégítő biztonságú operációs rendszerrel használhatóak.
- Biztosítani kell az adatszinkronizálást a Középiskola központi rendszere és az aktuális felhasználás között.
- A külső munkahelyen történő felhasználás után az eszközökről az adatállományokat el kell távolítani.

8.3.7 Vezetéknélküli-hálózat használatának szabályai (Wi-Fi)

A Középiskola területén levő WiFi Access point-ok nem nyilvánosak, alapvetően csak a Középiskola tulajdonát képező mobil eszközök használhatják. Ez alól kivétel csak a Középiskola informatikai munkaközösség vezetőjének egyedi engedélyével rendelkező mobil eszközök (pl. tanárok otthoni saját hordozható eszközei).

A wifi hálózat elérése kóddal védett (Open Shared Key - Nyílt hálózati kulcs, 128 bites) valamint az Access Point-ok MacAddress szűrést alkalmaznak, tehát csak azok a hordozható eszközök vehetnek részt a hálózati kommunikációban, amelyek MacAddress címét a rendszergazda ismeri és beállította az eszközökön.

8.3.8 Energiaszolgáltatás biztosítása

A Középiskola a felszerelések védelmét az energia-kimaradással, valamint az egyéb elektromos meghibásodásokkal szemben szünetmentes tápegységekkel biztosítja.

A kiemelt fontosságú berendezéseket (szerverek, kapcsolóeszközök) szünetmentes tápegységekkel (UPS) védi, illetve néhány helyiségben található külön UPS is.

A szünetmentes tápegységek teszteléséről, kapacitásának ellenőrzéséről a Középiskola megfelelő időszakonként a gyártó ajánlásai szerint gondoskodik.

8.4 Az adatfeldolgozás folyamatához kapcsolódó intézkedések

8.4.1 Archiválás

Biztosítani kell, hogy a tárolóeszközökön levő programok, és adatállományok listája mindig az érvényes állapotot tükrözze vissza. Ezt a dokumentumot a biztonsághoz kapcsolódó többi dokumentummal együtt, azokkal azonos biztonsági szinten kell őrizni.

Dokumentumba kell foglalni, hogy mely adatállományok és programok nem megváltoztathatók. A változtatást lehetőleg a tárolóeszközön kialakítható fizikai írásvédelemmel kell megakadályozni.

Az elektronikus dokumentumokat oly módon kell megőrizni, amely kizárja az utólagos módosítás lehetőségét, a törlési határnapig folyamatosan biztosítja a jogosultak által a hozzáférhetőséget, valamint az elektronikus dokumentumok értelmezhetőségét (olvashatóságát). Az elektronikus dokumentumokat védeni kell a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés ellen.

Archiválás havonta egyszer történik. Az archiválás pontos menetrendjét a rendszergazda külön szabályozza.

8.4.2 Feldolgozás

A feldolgozások aktivizálásának jogát be kell vonni az azonosításhoz és hitelesítéshez, valamint a hozzáférési jogok vezérléséhez kapcsolódó szabályozásba. Egyértelműen definiálni kell, hogy milyen ügykörben, melyik személy milyen feldolgozási funkciókat

gyakorolhat, milyen ellenőrzési funkciókat végezhet el, és mely adatokhoz férhet hozzá a feldolgozás során.

A feldolgozáshoz kapcsolódó eseményeket a biztonsági naplózásnál előírt paraméterekkel rögzíteni kell, és kérésre ki kell tudni listázni utólagos ellenőrzés céljából. Ebből egyértelműen ki kell derülnie annak, hogy ki, mikor, milyen feldolgozást végzett.

A feldolgozáshoz kapcsolódóan csak olyan adatmásolási, mentési feladatokat szabad elvégezni, amelyek a feldolgozási feladatkör teljesítéséhez szükségesek és nem sértenek egyéb, a Szabályzatban meghatározott intézkedéseket. A jogosultsági rendszer felállításakor figyelmet kell fordítani az illetéktelen másolások megakadályozására.

9. Katasztrófaterv

9.1 Bevezetés

Ez a katasztrófa-elhárítási terv csak azokkal a feladatokkal foglalkozik, amelyek egy átfogó informatikai biztonsági szabályozás kereteiben kimondottan a katasztrófa-elhárítás témakörébe tartoznak.

A katasztrófa-elhárítási terv, illetve az abban foglalt eljárási szabályok feladata, hogy elvárható mértékben biztosítsa egy esetlegesen bekövetkező katasztrófaesemény megelőzését, illetve az abból eredő károk minimalizálását, a következmények minél hamarabbi elhárítását.

9.2 Meghatározások

A katasztrófa-elhárítási terv öt részből áll:

- a katasztrófa-elhárítási terv definíciója,
- a mentési (megelőzési) terv,
- a helyreállítási terv,
- tesztelési terv,
- a karbantartási (üzemben tartási) terv.

Az informatikai rendszer katasztrófája egy olyan esemény, amely a rendszer adatfeldolgozó képességének részleges vagy teljes elvesztését okozza hosszabb időre. **A katasztrófa-elhárítási terv** definíciószerűen meghatározva eljárások vagy tevékenység-lépések sorozata, annak biztosítására, hogy a Szervezet kritikus információfeldolgozó képességeit helyre lehessen állítani

- elfogadhatóan rövid idő alatt,
- a szükséges aktuális adatokkal,

egy katasztrófa bekövetkezése után.

A mentési terv azon lépések sorozata, amelyeket azért kell végrehajtani a katasztrófát megelőzően (a normál üzem során), hogy lehetővé tegyék a szervezet számára a reagálást egy katasztrófa bekövetkezésére. A mentési terv végrehajtásával lehet eszközöket biztosítani a helyreállításhoz.

A helyreállítási terv olyan eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy az informatikai rendszert egy tartalék központban helyreállítsák, vagy helyreállítsák az adatfeldolgozó központot.

A tesztelési terv azokat a tevékenységeket tartalmazza, amelyek a katasztrófa-elhárítási terv működőképességét ellenőrzik és biztosítják.

A karbantartási tervet használjuk a katasztrófa-elhárítási terv aktuális állapotban tartására, a szervezet változásainak követésével.

A katasztrófa-elhárítási tervben az alábbiak kerülnek meghatározásra:

1) rendelkezésre állási követelmények felállítása;
2) a katasztrófa vagy vészhelyzet események definíciója;
3) a korlátozott informatikai üzem fogalma (visszaesési fokozatok) és a hozzájuk tartozó funkcionalitási szintek;
4) javaslat a felelősségek szabályozására veszély vagy katasztrófa bekövetkezése esetén;
5) kiválasztott esetekre konkrét intézkedési terv, különösen az alábbi területen:
   - a szükséges hardver és szoftver konfiguráció rögzítése szükségüzem esetére, beleértve az adatokat is,
   - amennyiben lehetséges, manuális póteljárás rögzítése a szükségüzem esetére,
   - szükség esetén backup-rendszer (például saját vagy külső tartalék központ),
   - adatrekonstrukciós eljárások kidolgozása és bevezetése,
   - újraalkalmazhatóvá tevő intézkedések,
   - az olyan informatikai rendszerek védelme, amelyeknek állandóan elérhetőeknek kell lenniük (például redundancia intézkedésekkel és a hibákat toleráló hardverekkel és szoftverekkel),
   - az adatbiztosítási intézkedések megvalósítási szabályainak összeállítása (például háromgenerációs elv),
   - az üzemi szempontból szükséges adatok biztonsági kópiáinak elkészítése rögzített időszakonként,

- a biztonsági másolatoknak megfelelő helyen, de mindenképpen a munkaterületen, illetve a számítógépközponton kívüli raktározása,
- az installált rendszerszoftverek és a fontosabb alkalmazói szoftverek referenciamásolatainak biztonságos raktározása,
- a fontosabb dokumentációk megkettőzése és raktározása,
- a megvalósított adatbiztosítás ellenőrizhető dokumentációja;

6) visszaállítási terv, amely magában foglalja az informatikai alkalmazások prioritásainak kijelölését és a célkitűzések megállapítása (például az X alkalmazás újraindítása Y napon belül);
7) követelmények beszállítói (szolgáltatói) szerződésekre katasztrófa események esetében, hogy katasztrófa helyzetben is biztosítani lehessen a rendelkezésre állást;
8) javasolt biztosítások katasztrófák, káresemények esetére.

Az intézkedések az alábbi területekre terjednek ki:

- intézkedések a kármegelőzésre és minimalizálásra (pl.: belső vagy külső háttér, illetve tartalék számítógép-kapacitás előkészítése szükségüzem esetére a szükséges hardver és szoftver konfiguráció rögzítésével.);
- intézkedések a katasztrófák, veszélyhelyzetek bekövetkezésekor;
- intézkedések a katasztrófákat, káreseményeket követően a visszaállításra;
- intézkedés veszélyhelyzetek, katasztrófák eset-szimulálására, begyakorlásra, intézkedések kipróbálására.

A mentési tervnek kell tartalmaznia a különböző rendszerek mentésére vonatkozóan

1) A mentendő rendszerek meghatározását (név, egyéb jellemző)
2) A mentőeszköz meghatározását
3) A mentések gyakoriságát
4) A mentést tartalmazó adathordozók tárolási helyét
5) A mentések végrehajtásáért és az ellenőrzésekért felelős személyek kijelölését

A katasztrófa bekövetkezte utáni helyreállítási terv hat szakaszból áll:

1) Azonnali reakció: válasz a katasztrófa-helyzetre, a veszteségek számbavétele, a megfelelő emberek értesítése és a katasztrófa-állapot megállapítása.
2) Környezeti helyreállítás: Az adatfeldolgozó rendszer helyreállítása: operációs rendszer, program termékek és a távközlési hálózat.
3) Funkcionális helyreállítás: Az informatikai rendszer alkalmazásainak és adatainak helyreállítása, az adatok szinkronizálása a tranzakció naplóval.
4) Helyreállítás: Az elvesztett vagy késleltetett tranzakciók ismételt bevitele. Az üzemeltetők, a rendszeradminisztrátorok, az alkalmazók és a végfelhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet.
5) Áttelepülés: Az informatikai rendszer kiépítése a hidegtartalék létesítményben, ha a melegtartalék létesítmények használata időben korlátozott.
6) Normalizáció: Az új állandó informatikai rendszer kiépítése és arra az üzemelő rendszer áttelepítése.

A karbantartási tervet használják a katasztrófa-elhárítási terv aktuális állapotban tartására, a szervezet változása esetén. Ennek megfelelően a katasztrófa tervet három lehetséges esetben kell módosítani:

1) szervezeti változás esetén módosításokat kell alkalmazni, amennyiben ez érinti a felelősségi köröket,
2) az informatikai rendszer logikai terveinek változása esetén módosítani kell a mentési és a helyreállítási tervet is, amennyiben a változás érinti a szervereket (bővül, vagy csökken a szerverek száma, változik valamely szerver funkcionalitása).
3) ha a tesztelési dokumentáció értékelése előírja, módosítani kell a mentési és a helyreállítási tervet is. Ez akkor fordulhat elő, ha a tesztelés során kiderül, hogy a rendszer nem állítható helyre az előírások betartása mellett sem. Ekkor szükség szerint módosítani kell a terve(ke)t, attól függően, hogy mi okozta a hibát, ezt követően a tesztelést meg kell ismételni.

A katasztrófa-elhárítási tervet rendszeresen kell ellenőrizni, és a megváltozott körülményekhez igazítani.

9.2.1 A Középiskola katasztrófa-elhárítási tervének definíciója

A Középiskola katasztrófa-elhárítási terve olyan eljárások és tevékenység-lépések sorozata, amelyek segítségével az iskola folyamatai szempontjából kritikus információ-feldolgozó képességeit helyre lehet állítani, az iskola számára elfogadhatóan rövid idő alatt, a szükséges aktuális adatokkal, egy katasztrófa esemény után, amelynek következtében a Középiskola adatfeldolgozó képessége hosszabb időre elveszik.

9.2.2 Rendelkezésre állási követelmények felállítása

Az informatikai biztonsági szabályzat 2.2 pontja szerinti informatikai rendszereket alkalmazza a iskolai munka támogatására.

A mellékletben szereplő táblázatban a prioritások a következőket jelentik a Középiskola szempontjából:

0. = kritikus, azonnali helyreállítás szükséges, a helyreállítás megkövetelt válaszideje 8 óra

1. = "késleltetett" helyreállítás szükséges, a helyreállítás megkövetelt válaszideje 24 óra

2. = nem kritikus, a rendszer működőképességének helyreállítását a rendszerek teljes helyreállítása során elegendő biztosítani

A rendelkezésre állási követelmények meghatározásánál elsődleges szempont az iskolai munka folytonosságának, és az oktatás kiszolgálásának biztosítása. A központi, több szervezeti egység által, alkalmazott rendszerek, valamint a kapcsolattartást biztosító rendszerelemek kiesése kritikus eseménynek minősül.

9.2.3 A katasztrófa vagy vészhelyzet események meghatározása

A középiskola informatikai rendszereinek katasztrófa illetve vészhelyzet eseményeinek meghatározásakor a rendszerek sajátosságaiból kell kiindulni.

A veszélyforrások közé tartoznak

- a tűz, víz vagy természeti csapás által okozott károk,
- tudatos rombolás és eltulajdonítás,
- rendszer szoftver, hardver, áram vagy egyéb környezeti kiesés.

A Középiskola alapvető központi informatikai erőforrásai egy helyen, a szerverszobában kerültek elhelyezésre. Ebből eredően tehát kiemelt kockázatot jelent a tűz, az áramszolgáltatás kimaradása/kiesése, a tudatos rombolás és/vagy eltulajdonítás. Egy, a szerverszobában bekövetkező tűzeset akár a teljes központi informatikai rendszer (beleértve a külső kommunikációs hálózathoz csatlakozó eszközöket, a tűzfalat, és a teljes szerverparkot is!) megsemmisülését is eredményezheti.

A kommunikációs hálózati irányból (internet) a Középiskola informatikai rendszerei önálló tűzfalrendszerrel védettek. Ezen a területen kockázatot a tűzfalrendszer meghibásodása, illetve megsemmisülése jelent.

9.2.4 A korlátozott informatikai üzem fogalma

Katasztrófa, vagy vészhelyzet bekövetkezésekor egyes kiemelten fontos alrendszerek szolgáltatásainak azonnali (e katasztrófa-elhárítási terv meghatározása szerint 0. prioritású) működésének helyreállítása szükséges, korlátozott teljesítménnyel.

Korlátozott informatikai üzemnek tekintjük a rendszerek elégséges kapacitású eszközökön történő üzemeltetését, a feltétlenül szükséges hálózati kapacitások és kommunikációs sávszélességek biztosításával.

A korlátozott informatikai üzem lehetséges változatai Középiskolánál:

- Saját területen megvalósítva, tartalék eszközök biztosításával

Biztosítandó feltételek:

a.) terület
b.) infrastruktúra csatlakozási felületek (elektromos áram, LAN, kommunikáció)
c.) eszközök (szerverek

- Bérelt területen, a bérbeadó által biztosított eszközök felhasználásával

A bérbeadó szerződésben vállalja valamennyi, a korlátozott informatikai üzemhez szükséges eszköz azonnali biztosítását katasztrófa vagy vészhelyzet bekövetkezésekor.

9.2.5 A felelősségek szabályozása

Egy bekövetkező katasztrófa vagy vészhelyzet esetén a katasztrófa-elhárítás szigorúan hierarchikusan szervezett vezetési-felelősségi struktúrát igényel.

A katasztrófa-elhárítási bizottság háromtagú:

- A **Katasztrófa-elhárítási vezető** a szervezet egyszemélyi felelős vezetője, a feladatot a Középiskola igazgatója látja el.
- Az **Informatikai biztonsági vezető** a katasztrófa-elhárítási szervezetben konzultációs, operatív irányítási valamint kapcsolattartási feladatokat lát el.
- Az **Informatikai munkaközösség vezető** felelős általánosságban az informatikai katasztrófa-elhárítási munkákért.

A katasztrófa-elhárítás munkái során, a részfeladatok irányítására ki kell jelölni két további felelőst:

- Hardver, hálózati szolgáltatások helyreállítás vezetője, az alábbi feladatok megoldásának operatív irányítója
- Szoftver, szolgáltatások helyreállítás vezetője, az alábbi feladatok megoldásának operatív irányítója

9.3 Intézkedési terv kiválasztott esetekre

Az alábbi három terület működőképességének folyamatos fenntartása, vagyis egy katasztrófa bekövetkezésekor a szolgáltatások haladéktalan újraindítása kiemelten fontos az iskola szempontjából a következő rendszereknél:

- Gazdálkodási rendszer
- Portál

A megelőzéssel egyenértékű, egy katasztrófa bekövetkezésére való felkészülés az alábbi lépésekből áll:

- Tartalék eszközök meghatározása, kijelölése, fenntartása
- Telepítési hely kijelölése, kialakítása, fenntartása
- Korlátozott üzem kialakításának megtervezése (részletes tevékenységlista az áttelepüléshez)

9.4 Tevékenység-sorozat katasztrófa bekövetkezése esetén

Kiindulás: a katasztrófaesemény bekövetkezte

Tevékenységek:

- Az esemény felismerése
- Beavatkozás az esemény megállítására
- A katasztrófa-elhárítási csapat riasztása
- A károk enyhítése
- A helyreállítási folyamat megindítása
- Az alaptevékenységek visszaállítása
- Tényleges helyreállítás
- A tanulságok levonása

9.5 Mentési (megelőzési) terv

A szervereken tárolt adatokról automatikus napi mentés készül. A mentésekért felelős rendszergazda a központi szerverek teljes adattartalmáról napi, heti és havi (ún. 3 generációs) mentéseket készít.

A mentéseket a fenti bontásban (mentési generációnként külön oldalakon), a mentés tárgyának, a mentést tartalmazó objektumok/adathordozók megnevezésének (azonosító feliratának) és a mentés időpontjának feljegyzésével, külön *mentési füzetekben* a mentést végző személyeknek kell vezetni.

A felelős informatikus köteles esetenként a mentések elvégzését és megbízhatóságát ellenőrizni. Az adatmentéseket tartalmazó adathordozókat és a mentési füzeteket (naplókat) a szerver szobán kívül, lemezszekrényben vagy páncélszekrényben kell tárolni.

A felhasználók a saját munkaállomásuk merevlemezére írt fájlok mentéséről saját hatáskörben gondoskodnak, úgy hogy amennyiben azokat megőrzésre érdemesnek tartják újraírható optikai adattárolóra írják.

A fenti intézkedésen túlmenően, minden szerverre vonatkozóan archiválás, illetve mentés esetén be kell tartani az adott szerverre vonatkozó mentési rendet, majd az

adatokról másolati példányt kell készíteni (az informatikai munkaközösség vezető által meghatározott rendszeres időközönként), és azt biztonságosan kell elhelyezni.

Felelősök:

A mentések rendszeres és előírásszerű elvégzéséért a **szerverek rendszergazdái**, és a szerver rendszergazdáit koordináló személy (informatikai irodavezető) felelősök. A mentések dokumentálását a 8.2.3 pontban meghatározott módon kell vezetni.

A mentések dokumentálását az információvédelmi megbízott rendszeresen, a mentések tényleges elvégzését szúrópróbaszerűen ellenőrzi.

9.5.1 A különböző rendszerek mentési, archiválási rendje:

Mentendő rendszer megnevezése	Mentő/archiváló eszköz	Mentés gyakorisága	Adathordozó tárolási helye	Megjegyzés
Iskolai Adatbázis	CD RW vagy DVD RW	Heti	Igazgatói iroda	
Felhasználói adatbázis	CD RW vagy DVD RW	Heti	Igazgatói iroda	
Levelezési adatbázis	CD RW vagy DVD RW	Heti	Igazgatói iroda	
Szerver Konfigurációs adatok	Merevlemez	Telepítés után	Külső szerver	
Felhasználói munkakönyvtárak	CD RW vagy DVD RW, illetve Merevlemez	Heti	Igazgatói illetve rendszergazda iroda	
Munkaállomások	Merevlemez	Telepítés után	Rendszergazda iroda	

9.6 A mentések általános leírása

9.6.1 Tartományvezérlő szerverek (Domain Contoller-ek)

Az adatok mentését heti rendszerességgel, munkaidőn kívül kell elvégezni. Az operációs rendszer konfigurációját külső telephelyen elhelyezett szerver merevlemezére kell menteni (így a rendszeradatok mellett a tartományhoz tartozó gépek és felhasználók adatai, valamint a hozzáférési, jogosultsági adatok is mentésre kerülnek). A mentés várható időtartama 2 óra.

Ezen felül heti rendszerességgel „repair disk”-et kell készíteni a szerverekről (a „repair disk”-en is tárolásra kerül a felhasználói adatbázis), és a „repair disk”-et a mentésekkel együtt kell tárolni.

A mentéseket tartalmazó adathordozókat hőálló, biztonsági szekrényben kell tárolni. A tárolás helye: igazgatói iroda.

9.6.2 Alkalmazásszerverek mentésével kapcsolatos általános feladatok

A szerverek mentése két részből:

1. az operációs rendszer, illetve
2. a szerveren futó alkalmazás mentéséből áll.

Ad 1. Az operációs rendszer mentése:

Az adatok mentése heti rendszerességgel, munkaidőn kívül történik. Az operációs rendszer konfigurációját szalagos/kazettás adathordozóra kell menteni.

Ad 2. Az alkalmazások mentése:

Az adatok mentését napi rendszerességgel, a folyamatos működés során kell elvégezni rendszergazda jogokkal rendelkező felhasználó nevében.

9.6.3 Mentési specialitások

Portál szerver:

A mentési művelet során csak az adatbázis fájlok kerülnek lementésre, floppy lemezre, illetve a gépben található második merevlemezre, tömörítve.

Az adatok mentését napi rendszerességgel, a folyamatos működés során kell elvégezni rendszergazda jogokkal rendelkező felhasználó nevében.

Intézményi Munkaügyi Információs (IMI) rendszer mentése:

Az adatok mentését napi rendszerességgel, a folyamatos működés során kell elvégezni úgy, hogy a rendszergazda jogokkal felruházott felhasználó a mentés idejére kilépteti az éppen a rendszerben lévő többi felhasználót. A művelet során csak az adatbázis fájlok kerülnek lementésre, floppy lemezre, illetve a gépben található második merevlemezre, tömörítve.

A szerveren található intézményi munkaügyi és béradatok havi rendszerességgel feladásra kerülnek egy felügyeleti szerverre a Terület Államháztartási Hivatalhoz. Teljes katasztrófa esetén az adatok a TÁH-tól visszanyerhetők.

9.7 Helyreállítási terv

Egy katasztrófa bekövetkezése esetén az első dolog; amit végre kell hajtani, hogy fel kell mérni a károkat, és ennek megfelelően értesíteni kell az illetékes személy(eke)t, akik a helyreállítást el tudják végezni.

9.7.1 Környezeti helyreállítás:

A helyreállítás első lépéseként a fizikai környezetet kell helyreállítani: a meghibásodott rendszerelemeket ki kell javítani, illetve szükség esetén pótolni kell.

A javításhoz, illetve az eszközök pótlásához – a kár mértékétől függően – különböző eszközök beszerzésére van szükség. A Középiskola teljes informatikai infrastruktúráját érintő katasztrófa esetén a szervereket tartalmazó alhálózat önálló hálózatként bárhol létrehozható, amennyiben a hálózati aktív eszközök, és a számítógép-park pótlása megtörténik.

1) A hálózat helyreállítása:

A kiválasztott helyszínhez mérten meg kell tervezni, és el kell végezni a hálózati kábelezést, majd a kábeleket csatlakoztatni kell az aktív eszközökhöz, illetve a számítógépekhez.

2) A szerverek helyreállítása (operációs rendszerek):

A szerverek helyreállítása többféleképpen történhet:

Egyrészt a „tükör” winchesterek beszerelésével, másrészt újratelepítéssel.

Az első megoldás problémákba ütközhet a hardver elemek különbözősége miatt, de ha az eredeti és az új konfiguráció között nincs jelentős eltérés (*célszerű az IT nyilvántartásban szereplő konfiguráció figyelembe vételével megvásárolni a pótlásnak szánt számítógépet*), akkor egy kis hangolással gyorsan elérhetővé válnak az eredeti beállítások és adatok. Ennek különösen a tartományvezérlőknél van szerepe, mert a felhasználói és gépadatok nehézkesen állíthatók elő újra.

9.7.2 Az egyes szerverek helyreállítása

Tartományvezérlő szerverek (Primary és Backup Domain Controller -ek)

Az operációs rendszer helyreállítása után, a rendelkezésre álló legfrissebb mentési adatok szerverre történő visszatöltése következik. Ha ez a módszer nem vezet eredményre, akkor elő kell venni a „repair disk”-et, és azzal kell helyreállítani a szerver adatbázisait. Ezzel a művelettel gyakorlatilag az eredeti állapot helyreállítása fog megtörténni. Ha a tartományvezérlő szerverek helyreállítása megtörtént (*a hálózat működtetésének eléréséhez elegendő a Primary Domain Controller helyreállítása is, a BDC csak a PDC meghibásodása esetén nyer jelentőséget*), a többi szerver és a munkaállomások hálózatba csatlakoztatása is megkezdődhet.

A helyreállításhoz szükséges mentések, „repair disk”ek és ”tükör” példányok a mentési előírásoknak megfelelően a Középiskola titkárságán is megtalálhatók.

A bérszámfejtés központi szervere

Amennyiben a „tükör” módszerrel sikerült helyreállítani az operációs rendszert, úgy mindössze arra van szükség, hogy az IMI legfrissebb mentése visszatöltésre kerüljön, és a rendszer már működik is.

Amennyiben viszont csak telepítéssel sikerül az operációs rendszer helyreállítása, szükség lesz az IMI rendszer telepítésére is. Ezt a műveletet kizárólag a TÁH munkatársai tudják megtenni, mert csak ők rendelkeznek a telepítőkészlettel. Telepítés után be kell tölteni a legfrissebb verziót, amit szintén a TÁH-nál tudnak a FÖMI számára biztosítani, majd ha ez is felkerült a gépre, már csak a legfrissebb mentés visszatöltése szükséges, és a munka onnan folytatható, ahol félbeszakadt.

Egyéb szerverek helyreállítása két részből áll:

Az operációs rendszer helyreállítása:

Amennyiben a „tükör” módszerrel sikerült helyreállítani az operációs rendszert, akkor következhet a programrendszer helyreállítása, de ha csak telepítéssel sikerül az operációs rendszer helyreállítása, akkor a telepítésnél figyelembe kell vennünk, hogy a rendszert más alhálózatból is látni kell, ezért az eredetivel megegyező IP címet kell választani a szervernek.

A programrendszer helyreállítása:

Elő kell venni a legfrissebb mentést, és azt tetszőleges helyre vissza kell tölteni. Ez azért elegendő, mert a napi mentés mindig egy „dátum” könyvtárba történik, a teljes program másolásával, tömörítés nélkül. Ezután a legutolsó dátumnak megfelelő könyvtárból, annak egész tartalmát egy különálló winchesteren létrehozott könyvtárba kell másolni. Ezt a könyvtárat meg kell osztani, és ki kell adni a megfelelő jogosultságokat, a részlegvezető döntésének megfelelően. Végül a munkaállomásokon parancsikonokat kell elhelyezni, és el kell végezni a nyomtatási beállításokat. Amennyiben a Középiskola központi hálózatát is érintette a katasztrófa, szükség lesz a központban az átjárhatóságok konfigurálására, hogy a más alhálózatokból is elérhessék a szervert.

9.8 Tesztelési terv

A tesztelési terv azokat a tevékenységeket tartalmazza, amelyek segítségével a katasztrófa-elhárítási terv működőképességét ellenőrizni lehet.

A katasztrófa-elhárítási terv teszteléshez három számítógép, és egy hálózati eszköz (switch) szükséges. Ezek segítségével a Középiskola informatikai rendszerétől függetlenül, akár egy elkülönített helyiségben is lehetséges a rendszer helyreállításának tesztelésére. A fizikai eszközökön felül a teszteléshez szükséges a legfrissebb mentésekhez, és archív anyagokhoz való hozzáférés (Másolati példányok szükségesek, hogy az eredetiek a teszt során ne sérülhessenek).

A számítógépek mindegyikét ki kell jelölni a megfelelő funkciók betöltésére:

1. Tartományvezérlő
2. Bérszámfejtés központi szervere

3. A harmadik számítógép pedig egy munkaállomás szerepét látja el.

Ezután a gépeket a switch segítségével össze kell kábelezni, és a helyreállítási tervnek megfelelően el kell kezdeni a szerverek helyreállítását. Ezt követően a munkaállomás bekötésével le lehet tesztelni a szerverek funkcionális működését.

A tesztelés minden lépését megfelelően dokumentálni és értékelni kell. A tesztelést a részleg vezetőjének döntése szerinti gyakorisággal, rendszeresen végre kell hajtani. (Évente legalább egyszer teljes körű tesztelést kell végrehajtani.)

9.9 Karbantartási terv

A karbantartási terv azokat a lépéseket tartalmazza, melyek segítségével a katasztrófa-elhárítási terv mindig naprakész állapotban tartható.

Ennek megfelelően a katasztrófa tervet három lehetséges esetben kell módosítani:

1) szervezeti változás esetén módosításokat kell alkalmazni, amennyiben ez érinti a felelősségi köröket,
2) a hálózat logikai változása esetén módosítani kell a mentési és a helyreállítási tervet is, amennyiben a változás érinti a szervereket (bővül, vagy csökken a szerverek száma, változik valamely szerver funkcionalitása).
3) ha a tesztelési dokumentáció értékelése előírja, módosítani kell a mentési és a helyreállítási tervet is. Ez akkor fordulhat elő, ha a tesztelés során kiderül, hogy a rendszer nem állítható helyre az előírások betartása mellett sem. Ekkor szükség szerint módosítani kell a terve(ke)t, attól függően, hogy mi okozta a hibát. Ezt követően a tesztelést meg kell ismételni.

A tesztelési tervet rendszeresen kell ellenőrizni, és a megváltozott körülményekhez igazítani.

10. Mellékletek

10.1 Munkakörhöz kötött informatikai ismeretek

A Táncsics Mihály Szakközépiskola, ~~és~~ Szakiskola és Kollégium munkatársainak a betöltött munkaköröktől függően az alábbi informatikai ismeretekkel kell rendelkeznie

Munkakör	felhasz-nálói (MS Offi-ce, stb.)	szakirányú program	üzemel-tetői	progra-mozói	rendszer-gazda	rendszer-adminisztrá-tor
	ismeretek					
Titkárnő	x					
Ügyintéző	x	x				
Közép és felső vezető	x					
Adatbázis adminisztrátor	x			adatbázis, program-nyelvek	jogosultság, mentés	
Informatikus	x		hálózat, hardver	adatbázis, program-nyelvek		
Rendszeradmi-nisztrátor	x		hálózat, hardver	adatbázis, program-nyelvek	jogosultság, mentés	szerverek
Informatikai mun-kaközösség veze-tő	x	Internet	hálózat, hardver	adatbázis, program-nyelvek	jogosultság, mentés	szerverek

10.2 Munkatársi szoftverpolitikai nyilatkozat minta

Kitöltés után bizalmasan kezelendő, elzárt helyen őrzendő!

NYILATKOZAT

Alulírott: név: …….

cím: …….

A ……. dolgozója a

……munkahelyen (szoba száma, kirendeltség), a

…….típusú, ……gyári számú, ……leltári számú

számítógépet a következő számítógépi programokkal átvettem:

GÉP NEVE: ……. FELHASZNÁLÓ NEVE: …….

□ ……..operációs rendszer

□ ……irodai programcsomag

□ ……vírusvédelmi szoftver

□

Teljes anyagi és jogi felelősségem tudatában kötelezem magam arra, hogy a Táncsics Mihály Szakközépiskola, ~~és~~ Szakiskola és Kollégium szoftverhasználati politikáját és informatikai biztonsági előírásait betartom, ennek részeként a szerzői és szomszédos jogok által meghatározott rendelkezéseket betartom, a Középiskola számítógépére az Informatikai munkaközösség vezető engedélye nélkül számítógépi programot nem telepítek, le nem törlök, alapbeállításokat nem változtatok meg.

Kelt: ……., 201 .év hó nap

Aláírás

10.3 Munkatársi belépési nyilatkozat minta

Kitöltés után bizalmasan kezelendő, elzárt helyen őrzendő!

„Új belépő kommunikációs és IT szolgáltatási igénylő lapja”

Vezetéknév:	
Utónév:	
Leánykori név:	
Fogadó szervezeti egység:	
Belépés várható dátuma:	
Helyiség:	
Beosztás:	
Munkakör:	
Informatikai tudás / képzettség	

Felhasználói hálózati azonosító:	
E-mail cím elsődleges:	
Felhasználói csoport besorolás:	
Egyedi Informatikai igény:	

10.4 Katasztrófa-elhárítás - rendszerösszesítés

Rendszer	Iroda	Prioritás	Telepítés helye (Fizikai eszköz)	Minimális működés feltételei	Mentés eszköze	Megjegyzés
Domain Controllerek	Szerverszoba	1	HDD	AD és felhasználói adatbázis	Merevlemez	
Titkársági gépek telepítése	Titkárságok, gazdasági irodák	2	HDD	Gépek domainbe léptetve	HDD	
Iskolai adatbázis	Titkárságok, gazdasági irodák	3	HDD	Elérhető	CD RW, DVD RW	
Internet és Levelezés	Szerverszoba	4	HDD	Elérhető internet és működő levelező szerver	Merevlemez	
Levelezési adatbázisok visszaállítása	Szerverszoba	5	HDD	Régi levelek elérhetők	Merevlemez	
Munkaállomások	Tantermek, irodák	6	HDD	Domainba léptetve	HDD	

11. Fogalmak, meghatározások, értelmezések

A következőkben a Szabályzatban előforduló olyan fontosabb tárgyszavakat soroljuk fel, a hozzájuk tartozó értelmezésekkel, amelyek általában eltérnek a köznyelvi vagy más szakmabeli értelmezésektől.

Adatállomány

Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

Adatátvitel

Adatok szállítása összeköttetéseken, összekötő utakon (például számítógépek között).

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 jogszerűségeire 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.

Back-up rendszer

Az adatbiztosítás során az adatok rendelkezésre állását lehetővé tevő másolatokat őrző rendszer.

Bejelentkezés

Az informatikai rendszer és egy felhasználó között ez utóbbi által olyan kapcsolat kezdeményezése, amelynek során számára az informatikai rendszer funkcióinak használata lehetővé válik.

Bizalmasság

Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

Az információk vagy adatok esetében a bizalmasság azt jelenti, hogy azokhoz csak az arra jogosítottak és csak az előírt módokon férhetnek hozzá, és nem fordulhat elő úgynevezett jogosulatlan információszerzés. Ez vonatkozhat programokra, mint szélesebb értelemben vett információkra is (például ha valamely eljárás előírásait egy programmal írjuk le, és azt titokban kívánjuk tartani).

Bizonyítható azonosítás

A hozzáférési folyamat jogosultság ellenőrzése során olyan azonosítási eljárás, amelynek segítségével kétséget kizáróan, utólag is bizonyítható a felhasználó illetve a szolgáltatást igénybevevő kiléte.

Biztonság

Az információ és informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

Biztonsági mechanizmus

Eljárási módszer vagy megoldási elv, ami azt a célt szolgálja, hogy egy vagy több biztonsági követelményt teljesítsen. Így azután a biztonsági mechanizmusok az intézkedések részét képezik, ám egyben megvalósításukat is érintik.

Elérhetőség

Az információ-feldolgozás során valamely informatikai alkalmazás szolgáltatásai az adott helyen és az adott időben igénybe vehetők.

Felhasználó

Az a személy vagy szervezet, aki, (amely) egy vagy több informatikai rendszert használ feladatai megoldásához.

Felhasználói program (felhasználói szoftver)

Lásd: Alkalmazói program.

Féreg

Olyan programtörzs, amely a számítógép-hálózaton keresztül terjed és jut el egyik informatikai rendszerből a másikba és fejt ki "vírus" hatást.

Funkció

Az a lehetőség, amelyet valamely informatikai rendszer kínál, hogy egy meghatározott feladatot valamely informatikai alkalmazás keretében megoldjunk.

Hardver

Az informatikai rendszer eszközeit, fizikai elemeit alkotó részei.

Hálózat

Két vagy több számítógép vagy általánosabban informatikai rendszerek összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé.

Hitelesítés

Olyan eljárás, amelynek segítségével egy informatikai rendszeren belüli kapcsolatban a partnerek kölcsönösen kétségtelenül felismerhetik egymást és ez az állapot a kapcsolat egész idejére változatlanul fennmarad.

A továbbítandó információk hitelesítése azt tartalmazza, hogy az információk teljes egészében és változatlanul továbbítódnak, és a küldő ezt kétségtelenül megállapítja.

Hozzáférés

Olyan eljárás, amely valamely informatikai rendszer használója számára elérhetővé tesz a rendszerben adatokként tárolt információkat. Ez az eljárás bekövetkezhet például névmegadáson keresztül valamely adatszerűségre nézve, s lehetővé tehet olvasást, írást vagy kifejtést.

Informatika

A számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

Informatika-alkalmazás

Valamely informatikai rendszer olyan feladatok teljesítésére történő bevezetése, amelyek egy meghatározott, behatárolt szakmai és szervezeti területre esnek és közös jegyeik révén tűnnek ki, például

- szövegfeldolgozás az irodában,
- könyvelés a cégeknél,
- információk grafikus ábrázolása,
- program-előállítás a szoftvergyártóknál stb.

Informatika alkalmazó

Szabályozási értelmezésben informatikaalkalmazók lehetnek mind a felhasználók, mind az üzemeltetők. (Lásd még: felhasználó)

Informatikai biztonság

Az informatikai biztonság a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Egyszerűsítve: az informatikai rendszerekben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme.

Az informatikai biztonság tehát olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni.

Informatikus

Az a szükséges számítástechnikai ismeretekkel rendelkező személy, akit ezzel a feladattal a felettese írásban megbíz. Feladatai közé tartozik egyebek között a hardver és/vagy szoftver beszerzések és selejtezések, az informatikai nyilvántartások pontos, naprakész vezetése és ezek egyeztetése a területi leltárfelelőssel; a központi informatikai szolgáltatások (e-mail cím, IP cím, operatív beüzemelés, informatikai eszközigénylés) igénybevétele során kapcsolattartás és ügyintézés.

Informatikai rendszer

A hardverek és szoftverek olyan kombinációjából álló rendszer , amit az adat- illetve információ-feldolgozás különböző feladatainak teljesítésére alkalmazunk. Az informatikai rendszerek különleges tulajdonsága a szabad programozhatóság. Az informatikai rendszerek közé soroljuk tipikusan a "célszámítógépeket" és az "általános célú számítógépeket".

Informatikai rendszerek például

- nagyszámítógép ("main frame")
- részlegszámítógép,
- irodai rendszerek,
- munkahelyi számítógépek (személyi számítógépek, laptopok, mikro-számítógépek, munkaállomások),
- kommunikációs rendszerek (telekommunikációs berendezések, számítógép-hálózatok) stb.

beleértve a bevezetési célok elérését szolgáló szoftvereket, úgymint a rendszerprogramokat és az alkalmazói programokat.

Informatikai szolgáltatás

Valamely informatika-alkalmazás külön is definiált része, mint például egy zárt munkafolyamat, amelyet informatikai rendszerrel támogatnak.

Információ

Jelentéssel bíró szimbólumok összessége, amelyek jelentést hordozó adatokat tartalmaznak. Informatikai értelemben — azaz az informatikai rendszereken belül — az információk kódolva, adatok formájában fordulnak elő. Ahhoz, hogy az informatikai rendszerben tárolt adatokat ember számára érthetővé tegyük, át kell alakítani, vagy interpretálni, magyarázni kell azokat.

Információ-feldolgozás

Az adatfeldolgozás általános szinonimája, amely alatt értjük az információk

- begyűjtését,
- feltérképezését/feltárását,
- használatát,
- tárolását,
- továbbítását,
- programvezérelt feldolgozását (szoros értelemben) és
- ábrázolását.

Információrendszer

Információk meghatározott célú, módszeres gyűjtésére, tárolására, feldolgozására (bevitelére, módosítására, rendszerezésére, aggregálására) továbbítására, fogadására, megjelenítésére, megsemmisítésére stb. alkalmas rendszer. Ha ez a rendszer számítógéppel támogatott, akkor számítógépes információrendszerről (informatikai rendszerről) beszélünk.

Logikai bomba

A vírus olyan része illetve szerkezete, amelyik időhöz, esemény bekövetkezéséhez, logikai változó adott értékéhez kötött módon aktivizálódik.

Munkahelyi számítógép

Személyi számítógép, laptop vagy munkaállomás a munkahelyre telepítve.

Működőképesség

A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal. Ezen állapot fenntartásának alapfeladatait a rendszer adminisztrátor (rendszer menedzser) látja el.

Program

Eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.

Rendelkezésre állás

Az informatikai rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

Az a tényleges állapot, amikor is egy informatikai rendszer szolgáltatásai - amely szolgáltatások különbözők lehetnek - állandóan, illetve egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig

tartósan nincs akadályozva. Ebben az összefüggésben jelentősége van az információ vagy adatok rendelkezésre állásának, elérhetőségének is.

Rendszerprogram (rendszer szoftver)

Olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

Sértetlenség, integritás

Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

A sértetlenséget általában az információkra, adatokra illetve a programokra értelmezik. Az információk sértetlensége alatt azt a fogalmat értjük, hogy az információkat csak az arra jogosultak változtathatják meg és azok véletlenül sem módosulnak. Ez az alap veszélyforrás a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani. A sértetlenség fogalma alatt gyakran értik a sérthetetlenségen túli teljességet, továbbá az ellentmondásmentességet és a korrektséget, együttesen: integritást. Az integritás ebben az összefüggésben azt jelenti, hogy az információ valamennyi része rendelkezésre áll, elérhető. Korrektek azok az információk, amelyek a valós dologi vagy — pl. modellezésnél — feltételezett állapotot helyesen írják le.

Szoftver

Valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

Támadás

Valamely személy (tettes) akciója azzal a szándékkal, hogy valamely informatikai rendszert veszélyeztessen, és károkat okozzon.

Trójai program

Olyan programtörzs, amelyeket készítője illegálisan épített be az általa tervezett programba és a felhasználó szándéka ellenére és tudta nélkül hajt végre illegális feladatokat (adattörlés, illegális lemezművelet, program megsemmisítés, stb.).

Védelmi mechanizmusok

Olyan védelmi intézkedések, amelyeket biztonsági szabványok határoznak meg a hardver, és szoftver gyártó cégek pedig termékeik előállítása során építik be és szolgáltatják a felhasználók részére.

Zárt védelem:

Zárt a védelem, ha az az összes releváns fenyegetést figyelembe veszi.

Teljes körű védelem:

Teljes körű a védelem, ha az az informatikai rendszer összes elemére kiterjed.

Folytonos védelem:

Folytonos a védelem, ha az az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

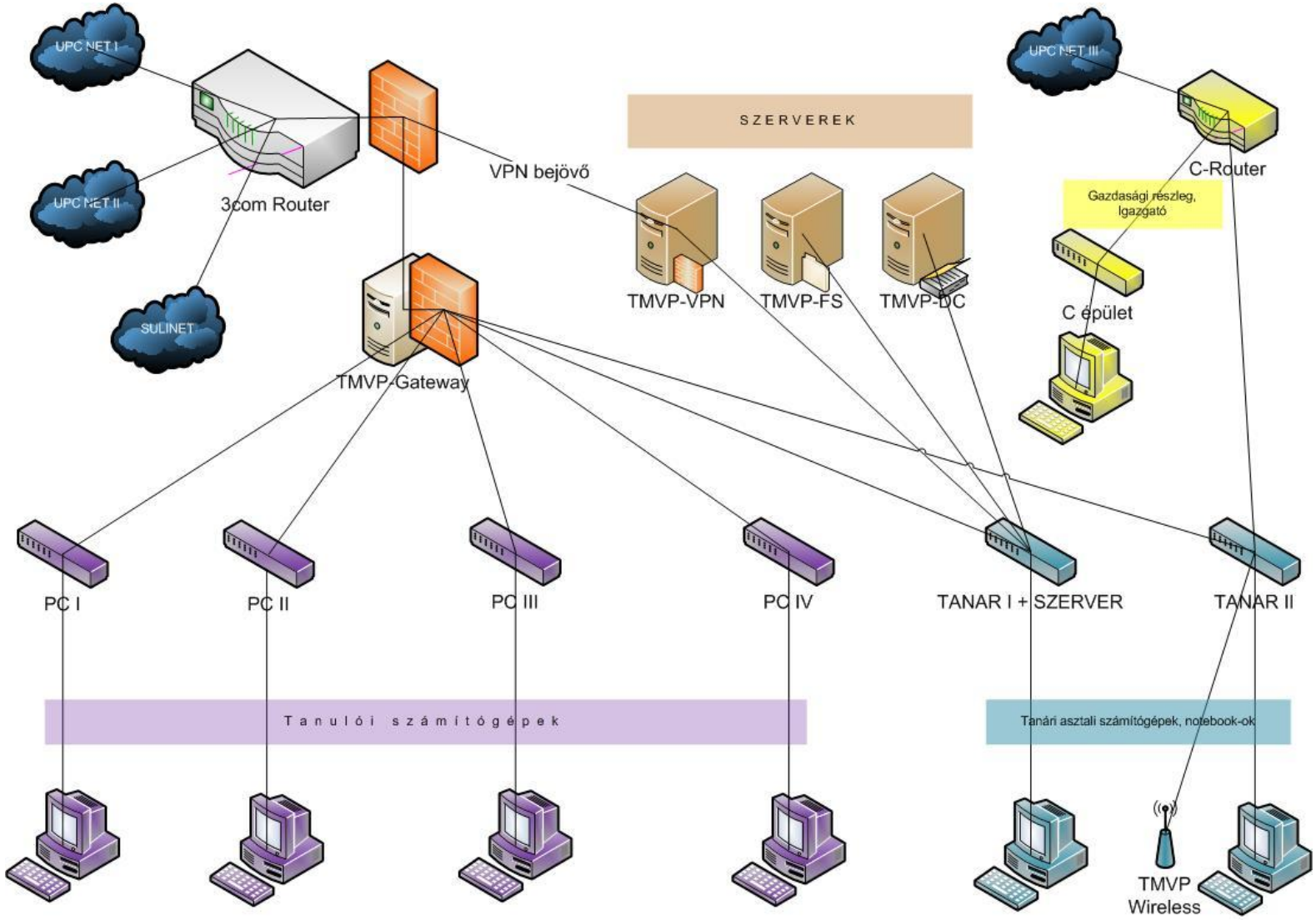
Kockázattal arányos védelem:

A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

Vírus

Olyan programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer- illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl.: konkrét időpont, szabad lemezterületi helyek száma, stb.) Trójai faló hatást indít el.

12. A Középiskola számítógéphálózatának logikai vázlata



12. Megismerési Nyilatkozat

Az Informatikai Biztonsági Szabályzat és Katasztrófa elhárítási tervben foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani és betartatni.

Név	Beosztás	Keltezés	Aláírás
Eveli Péter	igazgatóhelyettes		
Hajduné Medgyesi Andrea	igazgatóhelyettes		
Krausz Attila	igazgatóhelyettes		
Varga Gyula	tanműhelyvezető		
Pataki Imre	rendszergazda		
Filipovits Lajos	rendszergazda		
Kiss Ernő	rendszergazda		

13. Záró rendelkezések

A szabályzat időbeli és személyi hatálya:

A szabályzat kiterjed az intézmény valamennyi dolgozójára.

Jelen szabályzat **2011. február 28.** napjával lép hatályba és ezzel egyidejűleg minden korábbi, ide vonatkozó belső utasítás hatályát veszti.

A szabályzat hozzáférhetősége és módosítása

A szabályzat munkatársakra vonatkozó részeit az intézményvezető helyettesei kötelesek ismertetni a beosztott munkatársakkal.

A szabályzat egy példányát hozzáférhetővé kell tenni az intézmény valamennyi dolgozója számára a gazdasági vezető irodájában.

A szabályzatot módosítani kell, ha az intézmény sajátosságai, működésének változása, illetve jogszabályi változás alapján indokolttá válik.

Veszprém, 2011. február 28.

Körmendi István
igazgató