PÁPAI PETŐFI SÁNDOR GIMNÁZIUM

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

(2024. szeptember 01. napjától hatályos változat)

PÁPAI
PETŐFI SÁNDOR
GIMNÁZIUM

Készítette: Takács Mihály

rendszergazda

Tartalomjegyzék:

1. Az Informatikai Biztonsági Szabályzat célja

(1) Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az intézménynél az elektronikus biztonság, és adatvédelem alkotmányos elveinek, követelményeinek az érvényesülését, és megakadályozza a jogosulatlan hozzáférést, megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

(2) Az Informatikai Biztonsági Szabályzat célja továbbá:

a. a titok, munka, vagyon és tűzvédelemre vonatkozó védelmi intézkedések betartása,

b. az üzemeltetett informatikai rendszerek rendeltetésszerű használata,

c. a biztonságot szolgáló karbantartás és fenntartás,

d. az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,

e. az adatállományok tartalmi és formai épségének megőrzése,

f. az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,

g. a munkaállomásokon lekérdezhető adatok körének meghatározása,

h. az adatállományok biztonságos mentése,

i. az informatikai rendszerek zavartalan üzemeltetése,

j. a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,

k. az adatvédelem és adatbiztonság feltételeinek megteremtése.

(3) A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

(4) A jelen Informatikai Biztonsági Szabályzat az elektronikus védelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

(l) Az IBSZ személyi hatálya az intézmény valamennyi fő és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

3. Tárgyi hatálya:

a. kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, és az adatok fizikai megjelenési formájuktól függetlenül,

b. kiterjed az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,

c. kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),

d. kiterjed a rendszer, és felhasználói programokra,

e. kiterjed az adatok felhasználására vonatkozó utasításokra,

f. kiterjed az adathordozók tárolására, felhasználására.

4. Kapcsolódó szabályozások

(1) Az Informatikai Biztonsági Szabályzatot az alábbi előírással összhangban kell alkalmazni:

a. Szervezeti és Működési Szabályzat.

(2) Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

(3) Az informatikai rendszerre az alábbi tényezok hatnak:

a. a környezeti infrastruktúra,

b. a hardver elemek,

c. az adathordozók,

d. a dokumentumok,

e. a szoftver elemek,

f. az adatok,

g. a rendszerelemekkel kapcsolatba kerülő személyek.

(4) A védelem tárgya, a védelmi intézkedések kiterjednek:

a. a rendszer elemeinek elhelyezésére szolgáló helyiségekre,

b. az alkalmazott hardver eszközökre és azok működési biztonságára,

c. az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,

d. az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,

e. az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,

f. a személyhez fűződő és vagyoni jogokra.

(5) A védelem eszközei a mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

5. A védelem felelőse

(1) A védelem felelőse a rendszergazda, vagy akadályoztatása esetén annak, rendszergazdai szerződésben meghatározott megbízottja, erre kijelölt személy.

(2) A jelen szabályzatban foglaltak szakszerű végrehajtásáról a védelmi felelősnek kell gondoskodnia. Védelmi felelős feladatai:

a. ellenőrzi a védelmi előírások betartását,

b. felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,

c. gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,

d. feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,

e. a védelmi rendszer érvényesülésének ellenőrzése,

f. felelős az intézmény informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,

g. ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,

h. a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart, a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról, folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,

(3) A védelmi felelős, ellenőri feladatai:

a. rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,

b. előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

6. Az Informatikai Biztonsági Szabályzat alkalmazásainak módja

(1) A védelmet igénylő adatok, és információk osztályozása, minősítése, hozzáférési jogosultság.

(2) Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

a. közlésre szánt, bárki által megismerhető adatok,

b. minősített, titkos adatok.

(3) Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

(4) Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

(5) A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

(6) A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

(7) Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

(8) Minősített adatok esetén, az információhoz való hozzáférést a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység adatbázisokhoz való hozzáférés, a fájlba történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet utólag visszakereshető.

(9) A naplófájlokat havonta át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.

(10) A naplófájlok áttekintéséért, értékeléséért a rendszergazda felelős.

(11) A titkot képező adatok védelmét, a feldolgozás az adattovábbítás, a tárolás során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

(12) Kiosztott jogosultságok az intézményben használt szoftverekhez, adatokhoz

a. Könyvtár adatbázis (SZIKLA)

(13) A jogosultságok kiosztását megelőzően az érintett dolgozók adatbiztonsági nyilatkozatot írnak alá.

7. Az informatikai eszközbázist veszélyeztető helyzetek

(1) Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

(2) Környezeti infrastruktúra okozta ártalmak:

a. csőtörés,

b. földrengés, árvíz,

c. tűz,

d. villámcsapás, stb.

e. légszennyezettség,

f. a levegő nedvességtartalmának felszökése vagy leesése,

g. piszkolódás (pl. por).

h. feszültség kimaradás,

i. feszültségingadozás,

j. elektromos zárlat

(3) Emberi tényezőre vissza vezethető veszélyek:

a. Szándékos károkozás:

a) behatolás az informatikai rendszerek környezetébe,

b. illetéktelen hozzáférés (adat, eszköz), c) adatok, eszközök eltulajdonítása,

c. rongálás (gép, adathordozó),

d. megtévesztő adatok bevitele és képzése,

e. zavarás (feldolgozások, munkafolyamatok).

f. Nem szándékos, illetve gondatlan károkozás:

g. figyelmetlenség (ellenőrzés hiánya),

h. szakmai hozzá nem értés,

i. a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,

j. a jelszó gyakori, havonta történő megváltoztatásának az elmulasztása,

k. a megváltozott körülmények figyelmen kívül hagyása,

l. illegális másolattal vírusfertőzött adathordozó behozatala,

m. biztonsági követelmények és gyári előírások be nem tartása,

n. adathordozók megrongálása (rossz tárolás, kezelés),

o. a karbantartási műveletek elmulasztása.

(4) A szükséges biztonságjelző, és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

(5) Tervezés és előkészítés során előforduló veszélyforrások

a. a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,

b. hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

(6) Rendszerek megvalósítása során előforduló veszélyforrások

a. hibás adatállomány működtetése,

b. helytelen adatkezelés,

c. programtesztelés elhagyása.

(7) Működés és fejlesztés során előforduló veszélyforrások

a. emberi gondatlanság,

b. szervezetlenség,

c. képzetlenség,

d. szándékosan elkövetett illetéktelen beavatkozás,

e. illetéktelen hozzáférés,

f. üzemeltetési dokumentáció hiánya.

8. Az informatikai eszközök környezete, azok védelme

(1) Munkaállomások

A felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook). Asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkezd, hordozható elektronikus eszköz. Ide tartoznak: laptopok, notebookok, táblagépek, mobiltelefonok és okostelefonok. Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és az operációs rendszerből is kijelentkezett. A számítógépes munkaállomások képernyőit úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa. Munkaállomásokra vonatkozó előírást csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót bezárva kell tartani.

(2) Adathordozók

a. könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,

b. az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,

c. a használni kívánt adathordozót (CD, DVD, USB-memória , külső merevlemez) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,

d. a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,

e. adathordozót más szervezetnek átadni csak engedéllyel szabad,

f. a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

(3) Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetés, karbantartás és szervizelés rendjét külön utasításban kell szabályozni. A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni. A munkák szervezésénél figyelembe kell venni:

a. a gyártó előírásait, ajánlatait,

b. a hardver tesztek által feltárt hibákat.

c. billentyűzet, monitor, nyomtató cseréjének idejét dokumentálni kell

d. Alapgép szétbontását csak a rendszergazda végezheti el.

(4) Szoftver védelem

A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.

(5)Vírus védelem

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

a. Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.

b. A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát. Ha az adathordozón a vírusellenőrző program vírust talált, nem engedhet másolást, futtatást, amíg a vírusoktól nem mentesítik az adathordozót.

c. Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.

d. A felhasználók részéről tilos a vírusellenőrző szoftver beállításainak módosítása.

(6)Szerverszoba

A gépterem és szerverszoba védelme elemi csapás (vagy más ok) esetén a gépteremben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

a. menteni a még használható anyagot,

b. biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,

c. új adatfeldolgozás, helyiségek kialakítása,

d. archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

Fenttartási igénye:

a. a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,

b. a lehető legkevesebb nyílászáróval kell rendelkeznie,

c. váratlan áramkimaradás esetén a szervereket szünetmentes tápegységgel kell ellátni, mellyel az áramkimaradás folyamatosságát biztosítani lehet.

(7)Egyéb vagyonvédelmi előírások

a. a szerverszoba helységét biztonsági zárakkal kell felszerelni,

b. a szerverszobába való be és kilépés rendjét szabályozni kell,

c. csak az illetékes dolgozók tartózkodhatnak a gépteremben,

d. munkaidon túl a szerverszobában csak engedéllyel lehet dolgozni,

e. a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,

f. a szerverszobába történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,

g. az informatikai eszközöket csak a kijelölt dolgozók használhatják,

h. az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

(8)Tűzvédelem

a. A gépterem (szerverszoba) illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

b. A tűzvédelem feladatait, sajátos előírásokat a gépteremre vonatkozóan az intézmény Tűzvédelmi szabályzata tartalmazza.

c. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

d. Külön tűzszakaszt kell képezni a gépterem és az adatállománytároló helyiség között.

e. Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni. A gépteremben dohányozni tilos!

f. A géptermekben, valamint a munkaállomásoknál ételt, italt fogyasztani tilos!

g. A nagy fontosságú, pl. törzsadatállományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

9. Az informatikai feldolgozás folyamatának védelme

(1) Az adatrögzítés védelme

A szerverek rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontását dokumentálni kell. Rögzítési folyamatok meghatározása:

(2) Az adathordozók védelme és tárolása

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani. Az informatikai eszközök üzemeltetéséért a mindenkori rendszergazda felelős.

Köteles gondoskodni a feldolgozások igényeinek megfelelő mágneses adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

Az adathordozók tárolására a géptermen kívüli műszaki, és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

(3) Az adathordozók nyilvántartása

Az adathordozókról nyilvántartást kell vezetni. A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását. A nyilvántartás vezetéséért körzet leltárfelelőse a felelős.

(4) Az adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá intézményünk Bizonylati rendjében és Adatkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

(5) Selejtezés, sokszorosítás, másolás

Olyan mágneses adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell: a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan CD, DVD, merevlemez, USB-memória

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezésről jegyzőkönyvet kell készíteni, melynek az alábbi adatokat kell tartalmaznia:

a. a selejtezendő adathordozók tulajdonosának megnevezését,

b. a selejtezés időpontját,

c. milyen adathordozók, és azok mely adatai kerülnek selejtezésre,

d. a selejtezést végzők aláírását.

e. A selejtezési jegyzőkönyvek nem selejtezhetők.

f. Titkos adatokat tartalmazó adathordozókat selejtezni nem lehet.

g. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni.

h. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

(6) Leltározás

Az adathordozókat a Leltárkészítési és leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

(7) Mentések, fájlokok védelme

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.

a. A mentett adatokhoz csak a mindenkori rendszergazda, illetve az igazgató férhetnek hozzá.

Az egyéb mentéseket meghatározott időszakonként el kell végezni. Az adatokról biztonsági mentés készül NAS egységre, melynek tárolási helye nem lehet a szerverterem.

A munkák során létrehozott dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.

A levelezések biztonsági mentését a rendszergazda végzi el.

Az adatállományok filevédelme során gondoskodni kell arról, hogy azok ne károsodjanak.

A fontosabb állományokat tartalmazó adathordozókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

(8) Rendszerszoftver védelme

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára, amely szükség esetén azonnal betölthető legyen,

a. a rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges,

b. név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek,

c. a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni,

d. a változtatásokról nyilvántartást kell vezetni.

(9) Felhasználói programok védelme, Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Minden felhasználónak jelszóval kell védenie a használatban lévő számítógépét. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

A jelszavaknak az alábbi minimális követelménnyel kell rendelkeznie:

a. A hálózati jelszó legalább 8 karakterből álljon, kis és nagybetűk, valamint számok, egyéb írásjelek közül legalább 2 típusút tartalmazzon.

b. Az alkalmazáshoz szükséges jelszavaknak legalább 5 karakterből kell állni.

c. A jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, vagy könnyen visszafejthető kifejezéssel.

d. A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt 5 jelszóval.

e. A jelszót nem szabad több személy között megosztani.

f. A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.

g. A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.

Gondoskodni kell arról, hogy a tárolt programok, fileok ne károsodjanak, a követelményeknek megfelelően működjenek.

Lokális gépekre programot csak a rendszergazda tudtával lehet telepíteni.

A telepítést dokumentálni kell. A dokumentálásnak tartalmaznia kell azt, hogy milyen programot, mikor és ki telepített fel a számítógépre.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

a. a program azonosítója,

b. a program készítőjének neve,

c. a feldolgozási rendszer megnevezése.

A program dokumentáció a rendszerdokumentációnak része. Programok megőrzése, nyilvántartása, a programokról naprakész nyilvántartást kell vezetni, a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A programok nyilvántartásáért és működőképes állapotban való tartásáért a mindenkori rendszergazda felelős.

(10) Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezettségű dokumentálásnak. A dokumentációról nyilvántartást kell vezetni, s ennek az alábbiakat kell tartalmaznia:

a. rendszer megnevezése,

b. dokumentáció típusa,

c. a rendszer adatvédelmi minősítése,

d. a kidolgozók névsora,

e. példányszám és tárolás helye,

f. az átadás ideje,

g. módosítások megnevezése és ideje.

10. A központi eszközök, és a hálózat munkaállomásainak működésbiztonsága

(1) Központi gépek, szerver

Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek merevlemezei RAID1 tükrözéssel vannak ellátva. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

(2) Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell. Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad.

Új rendszereket használatba vételük elött szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A munkaállomások tekintetében az alábbi rendelkezéseket is be kell tartani:

a. A munkaállomások nincsenek jól védhető helyen, ezért védelmükről szoftver úton gondoskodni kell.

b. Ha a felhasználó napközben magára hagyja a gépet, zárolást, vagy jelszavas képernyővédőt kell alkalmaznia.

c. Ha a felhasználó munkaviszonya megszűnik, akkor felhasználói azonosítóját meg kell szüntetni.

(3) Hálózat védelme

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet. A hálózathoz való hozzáférés korlátozott. Az internet és a hálózat hibaelhárítása a mindenkori rendszergazda feladata. Hiba esetén az iskola vezetése azonnal értesíti a rendszergazdát.

11. Internet hozzáféréssel kapcsolatos intézkedések

(1) Az Internet eléréseket biztosító számítógépekre a helyi hálózatra nem kapcsolódó munkaállomásokra vonatkozó szabályok érvényesek.

(2) Az internetes gépen minden esetben működtetni kell a vírusvédelmet.

(3) A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.

(4) A tűzfal működése közben keletkező állományokat az üzemeltetőnek rendszeresen ellenőrizni kell.

(5) A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztését az igazgató felkérésére a rendszergazda szabályozza.

12. Elektronikus levelezéssel kapcsolatos rend

(1) Az elektronikus levelezést külső szolgáltató, külső szerver biztosítja. A szerveren alkalmazandó minimális biztonsági előírások:

a. rendelkezzen webes kliens alkalmazással

b. rendelkezzen az IBSZ-ben meghatározott jelszóházirenddel

c. rendelkezzen levelezési listák kezelésével

d. rendelkezzen olyan felülettel, mely segítségével különösebb szakértelem nélkül menedzselhetők az e-mail fiókok, listák

e. spam szűréssel rendelkezzen

f. rendelkezzen vírusvédelemmel

g. rendelkezzen rosszindulatú támadások elleni védelemmel

(2) Az alkalmazottak, munkavállalók esetleges munkahely váltása után az összes használt jelszót azonnal le kell cserélni!

(3) Az iskolai levelezést az arra jogosult felhasználók elérhetik Outlook levelezőprogramból és webböngészőből, az igazgató mobiltelefonon keresztül is, az elérhetőség biztosítása a rendszergazda feladata.

(4) A rendszergazda az iskolai levelezés mentését megadott időközönként elvégzi.

13. Jóváhagyási, egyetértési, véleményezési záradék

A Pápai Petőfi Sándor Gimnázium Diákönkormányzata és Intézményi Tanácsa a jelen szabályzatban foglaltakat megismerte, véleményezési jogát gyakorolta.

Pápa, 2024. augusztus 30.

....

Intézményi Tanács képviselője Diákönkormányzatot segítő pedagógus

A Pápai Petőfi Sándor Gimnázium nevelőtestülete a jelen szabályzatban foglaltakat 2024. augusztus 30-án tartott értekezletén elfogadta.

Pápa, 2024. augusztus 30.

....

Bognár Anita
igazgató

hitelesítő nevelőtestületi tag

A szabályzat felülvizsgálata megtörtént.

2025. február 27.

Bognár Anita

igazgató