Nyíregyházi Szakképzési Centrum
Zay Anna Technikum és Kollégium
4400 Nyíregyháza, Család u. 11.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Nyíregyháza, 2023. szeptember 1.

ÁLTALÁNOS RENDELKEZÉSEK

A szabályzat célja és hatálya

(1) Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) olyan normarendszer, amely a Nyíregyházi SZC Zay Anna Technikum és Kollégiumának az informatikai rendszerével kapcsolatos biztonsági intézkedéseit, előírásait tartalmazza. Az IBSZ belső használatra szóló dokumentum. Az intézményben kezelt adatok biztonsági osztályba sorolását az iskola Adatkezelési Szabályzata fogalmazza meg.

(2) Az IBSZ feladata továbbá, hogy az informatikai rendszereket érintő veszélyforrásokat felderítse, lehetővé tegye a szükséges kockázatelemzést, és meghatározza a védelmi intézkedéseket. A kockázat nagyságát – a bekövetkezés valószínűségét – és az esetlegesen okozott kár mértéket figyelembe véve három kockázati fokozat állapítható meg:

a) magas kockázati fokozat: az intézmény munkáját alapvetően befolyásoló kockázati tényezők, például a tartományvezérlő leállása, adatok megsemmisülése.
b) közepes kockázati fokozat: a központi szolgáltatások üzemeltetését befolyásoló kockázati tényezők, például a levelezés tartós kiesése.
c) alacsony kockázati fokozat: egyéb szolgáltatások üzemeltetését befolyásoló kockázati tényezők, például a WiFi hálózat rövid idejű meghibásodása.

(3) Az IBSZ feladata, hogy a kockázati fokozatokkal arányos védelem kialakítását lehetővé tegye. Ezen feladatának a biztonsági rendszer tervezésével tesz eleget. Az arányos védelem a védelemre fordítható anyagi lehetőségek, és a védeni kívánt érték vagy információ fontosságának függvényében alakul ki.

(4) Az IBSZ az intézmény informatikai tevékenységének átfogó szabályozására készített dokumentum. Célja, hogy az informatikai rendszer használata során biztosítsa a használhatóság és a biztonság együttes követelményeinek érvényesülését, megakadályozza a rendszerekhez való jogosulatlan hozzáférést, minimálisra csökkentse a szándékos vagy vétlen károkozást. Az IBSZ további célja, hogy a dolgozók és a diákok ismerjék az intézmény informatikai rendszerének használatát, a hálózat és a szolgáltatások használatából adódó kockázatokat, és elhárításuk rájuk vonatkozó részét.

(5) Az IBSZ célja, hogy az intézmény informatikai tevékenysége során kezelt eszközök, feldolgozott és továbbított adatok, illetve folyamatok bizalmasságát, sértetlenségét biztosítsa, valamint a rendelkezésre állást fenyegető veszélyek elhárítására védelmi intézkedéseket fogalmazzon meg.

(6) Az IBSZ célja továbbá, hogy megfogalmazza és szabályozza:

a) a titok-, vagyon-, tűzvédelemre vonatkozó védelmi intézkedéseket,
b) az üzemeltetett informatikai rendszerek rendeltetésszerű használatát,
c) az üzembiztonságot szolgáló járulékos szolgáltatások körét (klíma, szünetmentes áramforrás, stb.),
d) az adatállományok biztonságos mentését,
e) a speciális feladatokat ellátó helyiségek behatolás elleni védelmét.

(7) A szabályzat személyi és tárgyi hatálya:

a) A szabályzat személyi hatálya kiterjed. minden olyan személyre, aki használja az intézmény informatikai infrastruktúráját.
b) A tárgyi hatály érvényes a fizikai, infrastrukturális eszközökön kívül az adatok, szoftverek teljes körére.

(8) Az adatvédelem és adatbiztonság szabályozásával az intézmény Adatkezelési Szabályzata foglalkozik.

INTÉZKEDÉSEK

1.1. Felelősségi körök

(1) Az intézmény vezetésének feladata, hogy a szabályzatban megfogalmazott IT biztonsági szereplők részére a munkavégzésükhöz szükséges hatáskört és erőforrásokat biztosítsa.

(2) A rendszergazdák információbiztonsági kérdésekben közvetlenül az igazgatónak tartoznak beszámolási kötelezettséggel.

(3) Az intézmény dolgozói, tanárai, tanulói, egyéb felhasználói kötelesek betartani a jelen szabályzatban leírtakat, továbbá kötelesek jelenteni a rendszergazdáknak, ha biztonsági problémát okozó jelenséget (biztonsági incidens) észlelnek.

(4) A rendszergazdák feladata és felelőssége az információbiztonság szintjének folyamatos ellenőrzése, a biztonsági incidensek megelőzése, illetve a bekövetkező incidensek hatásának mérséklése, valamint az okok feltárása, a felelősök azonosítása, továbbá a későbbi beszerzések, az informatikai fejlesztések során a biztonsági követelmények érvényre juttatása.

(5) A rendszergazdák legfontosabb információbiztonsági feladatai:
a) az informatikai rendszereket fenyegető veszélyforrások miatt fellépő kockázatok meghatározása és csökkentése,
b) részvétel a védelmi rendszer tervezésében,
c) biztonsági szabályok meghatározása és betartatása,
d) a védelmi rendszer működtetésének és az intézmény informatikai biztonsági követelményeinek összehangolása,
e) az információ-biztonság rendszeres felülvizsgálata,
f) az informatikai hálózat biztonságának folyamatos ellenőrzése,
g) súlyos probléma esetén azonnali hibaelhárítás, akár iskolai munkafolyamatot megszakítva,
h) az informatikai rendszer változásainak nyomon követése, és ennek megfelelően módosítási javaslat kidolgozása,
i) az adatvédelmi felelőssel egyeztetve és együttműködve részt vesz a biztonsággal összefüggő szakmai munkában,
j) bejelentés alapján kivizsgálja a biztonsági incidenseket, és javaslatot tesz további intézkedésekre,
k) évente legalább egyszer ellenőrzi az IBSZ előírásainak betartását,
l) az előírások megszegőivel szemben felelősségre vonási eljárást kezdeményez.

(6) A rendszergazdák feladatát, felelősség- és hatáskörét a munkaköri leírás tartalmazza. A rendszergazda az információbiztonság szempontjából felelős:
a) a rábízott hálózat és eszközök biztonsági kockázatának minimalizálásáért,
b) az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismeréséért és jelentéséért,
c) az informatikai szabályok betartásáért.
d) biztonsági javítócsomagok telepítése,
e) biztonsági beállítások helyességének és sértetlenségének folyamatos biztosítása.

(7) A személyes használatban lévő számítógépek, hordozható számítógépek felhasználói biztonsági szempontból felelnek a rájuk bízott eszköz biztonságáért. Feladatuk:
a) biztonsági frissítések, javítócsomagok telepítése, jogtiszta szoftverek telepítése,
b) személyes jogosultság beállítása,
c) rájuk bízott érzékeny adatok védelme,
d) személyes használat megszűntekor vagy ellenőrzés céljából az eszközt eredeti szoftveres állapotában, illetve hardverelemei természetes elhasználódásának megfelelő állapotban visszaszolgáltatni.

1.2. Környezeti és fizikai biztonság

(1) Védett helyiségek: védettnek kell tekinteni azokat a helyiségeket, ahol a bizalmas adatok feldolgozására, tárolására alkalmazott informatikai erőforrások találhatók. A védett területek zárt területnek minősülnek, ezért védelmükről ennek megfelelően kell gondoskodni.

(2) Védett területnek minősül az intézményben:

a) az igazgatói iroda
b) az igazgatóhelyettesi irodák
c) a titkársági szoba
d) a gazdasági iroda,
e) a szerverszoba

(3) Szerverszoba: a szolgáltatásokat biztosító, szerver-feladatokat ellátó eszközöket közös helyiségben, szerverszobában kell elhelyezni. A szerver-helyiség biztonsági szempontból fokozottan védett helyiségnek minősül, melybe kizárólag ellenőrzött módon, az arra kijelölt személyek juthatnak be. A központi szerver-helyiséggel szemben támasztott követelmények:

a) zárt helyiség csak az arra feljogosított személyek léphetnek be,
b) szünetmentes áramforrás az üzembiztonság fokozása érdekében,
c) légkondicionálás az üzembiztonság fenntartása érdekében,
d) füst-, és tűzérzékelő a vagyonvédelem és az üzembiztonság érdekében.

(4) A szerverszobában végzendő munka szabályai:

a) a szerver helyiségbe csak arra feljogosított személy léphet be,
b) a szerver helyiségben munka csak feljogosított személy által vagy annak jelenlétében végezhető.

(5) A számítógép-használat általános alapelvei: az intézményben működő számítógépek csak rendeltetésszerűen, munkavégzés céljából használhatók. Minden felhasználó csak a munkájának végzéséhez szükséges rendszerekhez kaphat jogosultságot. Számítógépek használata során fokozott figyelmet kell fordítani a tűz-, érintés- és munkavédelmi szabályokra. A számítógépek és monitorok szellőzőnyílásait letakarni nem szabad, elektromos csatlakoztatások használata során kiemelt figyelmet kell fordítani az áramütés veszélyének megelőzésére. Informatikai hálózat csatlakoztatását megbontani nem szabad. Az intézményben működő számítógépekre csak az érvényes szabályozás mellett telepíthetők szoftverek. A beosztástól függően vagy a megbízott informatikai személy végzi a telepítést, vagy a személyes használatban lévő gép felhasználója. Azokban az esetekben, amikor a számítógép személyes használatban van, a felhasználó felelőssége, hogy gépére illetéktelen szoftver ne kerüljön fel, és az elemi biztonsági feltételeknek a számítógép megfeleljen.

(6) Informatika szaktantermek igénybevétele:

a) Órarendi igénybevétel: tanulók csak szaktanár felügyelete mellett és annak teljes felelősségére használhatják az iskola informatika szaktantermeit, az órarendi beosztásnak megfelelően, a következő kiemelt szabályok figyelembevételével:

- A helyiségek nyitása és zárása (kulcs felvétele és leadása a portán, aláírásával igazolva), áramtalanítása, valamint a felügyeleti szabályok betartása a szaktanár felelőssége.
- A felhasználók a munka megkezdése előtt ellenőrzik a számítógépüket: az áramellátást, a tartozékok állapotát, tisztaságát. Ha a felhasználó valamilyen rendellenességet tapasztal, köteles azonnal jelezni a problémát a szaktanárnak, aki értesíti a rendszergazdát.
- Minden felhasználó felelősséggel tartozik azon számítógépért, amelyen dolgozik: az eszközök állapotáért, tisztaságáért. Az eszközök csatlakozásait nem bonthatják meg, hardverek csatlakoztatását csak a rendszergazda engedélyével tehetik meg; kivételt képeznek a hordozható háttértárak, fejhallgatók.

- A felhasználók az informatika szaktantermekben – az eszközök állapotának megóvása érdekében – nem fogyaszthatnak ételt, italt, valamint nem tárolhatnak ételt, italt; kizárólag táskában, gondosan lezárva. Vizsgákon a terem végében – az informatikai eszközöktől legtávolabb – kialakított helyen megengedett étel és ital fogyasztása, valamint tanítási órákon ill. foglalkozásokon csak ital fogyasztása a megengedett a terem végében – az informatikai eszközöktől legtávolabb.
- A tanítási óra végeztével a felhasználók – munkájukat a megfelelő helyre elmentve – szabályosan leállítják a számítógépeket.

b) Egyéni igénybevétel: bárki, aki erre jogosult, csak tanulmányi vagy egyéb, az iskolai élettel összefüggő célra, az órarendi igénybevétel figyelembevételével használhatja az informatika szaktantermeket a következők betartásával: tanuló kizárólag tanári felügyelet mellett; dolgozó vagy tanár csak rendszergazdai, ill. igazgatói engedéllyel. Egyéni igénybevétel esetén is a felhasználókra és a felelős személyekre vonatkozó szabályok megegyeznek az órarendi igénybevétel szabályaival.

(7) Egyéb tanulmányi – nem adminisztratív – számítógépek igénybevétele:

a) Tanulók által:

az iskola informatika szaktantermein kívül található tanulmányi célra használható számítógépei kizárólag állandó szaktanári felügyelettel vehetők igénybe, a 2.2.6.b pontnak megfelelően. Ilyen rendeltetésű számítógépek találhatóak:

- a könyvtárban,
- a kollégiumi informatika szaktanteremben,
- az előadó termekben,
- demonstrációs szaktantermekben,
- egyes tantermekben.

b) Dolgozók ill. tanárok által:

- az egyes munkaközösségek irodájában található számítógépek kizárólag a munkaközösséghez tartozó szaktanárok által vehetők igénybe, felelősséggel a számítógépekért is ők tartoznak;
- a könyvtárban és a kollégiumi informatika szaktanteremben található számítógépeket bármely iskolai dolgozó igénybe veheti, az iskolai könyvtáros ill. kollégiumi nevelő felügyelete mellett;
- az anatómia előadóban található számítógépet (valamint projektortés interaktív táblát) az órarendi beosztásnak megfelelően bármely dolgozó ill. tanár igénybe veheti, jelezve azt a portai nyilvántartásban történő aláírásával, felveszi a kulcsokat, majd az óra végén leadja azt;
- a mikrobiológia előadóban található számítógépet (valamint projektort és interaktív táblát) az órarendi beosztásnak megfelelően bármely dolgozó ill. tanár igénybe veheti, melynek kulcsát a szakmai igazgatóhelyettestől veheti át, majd az óra végén leadja azt;
- a demonstrációs szaktantermekben található számítógépet az órarendi beosztásnak megfelelően bármely dolgozó ill. tanár igénybe veheti, melyek kulcsát a méregszobában lévő zárt szekrényből vehetik fel, majd az óra végén leadja azt;
- a tantermekben található számítógépet (valamint projektort és interaktív táblát) az órarendi beosztásnak megfelelően bármely dolgozó ill. tanár igénybe veheti, jelezve azt a portai nyilvántartásban történő aláírásával, felveszi a kulcsokat, majd az óra végén leadja azt.

(8) A felhasználóknak a személyes használatú munkaállomások használata során a következő általános szabályokat kell betartaniuk:

a) személyes használatban lévő számítógépen felhasználói jogokkal kell rendelkeznie,
b) felhasználói jogaihoz tartozó jelszóval védeni tudja számítógépe integritását,
c) illetéktelen személynek felhasználói jogát át nem adhatja,

d) közepes vagy magas biztonsági kockázattal járó feladat végzésekor a számítógépét senkinek át nem engedheti, információbiztonsági kockázatot nem okozhat,
e) működő számítógépet csak jelszóval védett képernyővédő használatával hagyhat magára,
f) csak jogtiszta szoftvereket használjon,
g) a gondatlan használatból eredő károkat köteles helyreállítani: az érintett hardverelem javítását vagy cseréjét szakemberrel elvégezteti, aminek anyagi felelőssége a felhasználóra hárul. Amennyiben vitatott, hogy rendeltetésszerű vagy gondatlan használat során keletkezett a kár, úgy az eszközt független szakértővel kell bevizsgáltatni, aminek költsége a felhasználóra hárul.

(9) A hálózat használatának szabályai:

Az intézményben strukturált és menedzselt informatikai hálózat működik. Ez a hálózat aktív és passzív elemekből áll. Illetéktelen személy a kialakított rendszeren nem változtathat, végpontot át nem helyezhet, és aktív vagy szerver-feladatokat ellátó eszközt a hálózatra nem kapcsolhat rá. A központi hálózat bővítésére vagy átalakításra kizárólag a rendszergazdák jogosultak.

(10) Az intézmény hálózata nem használható az alábbi tevékenységekre:

a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése),
b) profitszerzést célzó, direkt üzleti célú tevékenység és reklám,
c) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése,
d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. nem hivatali körlevelek, hálózati játékok, kéretlen reklámok),
e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata,
f) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység,
g) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok letöltése, közzététele),
h) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna

(11) A felhasználók kötelességei a hálózat használata során:

a) A felhasználók kötelessége a szabályzat megismerése és az abban foglaltak betartása, valamint együttműködni a hálózat üzemeltetőivel a szabályzat betartatása érdekében.
b) A felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználóhoz tartozó azonosítóval kerül végrehajtásra.

(12) A felhasználók jogai a hálózat használat során:

a) A felhasználónak joga van a felhasználói fiókhoz való hozzáféréshez. Az intézmény ezt a központi szolgáltatást a vezetőség, a tikárság és a gazdasági iroda dolgozóinak az asztali számítógépeiken, a tanároknak a tanári szobában és a kabinetekben elhelyezett számítógépeken, a tanulóknak pedig a számítógép-termekben, a könyvtárban és a kollégiumban teszi lehetővé.
b) A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetői tiszteletben tartják, ettől eltérni csak a törvény által meghatározott esetekben lehet.
c) A rendszer technikai problémáiról (tervezett vagy rendkívüli eseményekről) tájékoztatást kapjon.
d) A felhasználókra vonatkozó szabályok érvényes változatát megismerhesse.
e) A szervezeti egységek által biztosított további hálózati szolgáltatásokat igénybe vehetik.

(13) Jogosultságok kezelése a hálózat használata során:

a) Az eszközök használatának módját a felhasználói jogosultság szabályozza. A felhasználók különböző jogosultságokkal rendelkezhetnek, melyeket jelen szabályzat alapján, a meghatározott jogosultsági szinteknek megfelelően kell meghatározni.

b) A jelszavas védelemnek a szerverekre, a hálózatra kapcsolódó és a hálózati kapcsolat nélküli számítógépekre is ki kell terjednie. A felhasználói hálózatra érvényes jelszó nélkül senki nem kapcsolódhat. Gondoskodni kell a hozzáférések naplózásáról is, így regisztrálható a sikertelen hozzáférési kísérlet. Ha jogosulatlan hozzáférés történt, vagy a jogosulatlan hozzáférés gyanúja merül fel, a jelszót azonnal meg kell változtatni.

c) A hozzáférési jogosultságok meghatározásakor figyelembe kell venni az adatokat kezelő program, a biztonsági program biztonsági osztályba sorolását, az ellátandó feladatot és a feladatot végző személy felelősségi körét.

d) A jogosultság kiosztásakor alapelvként kell kezelni, hogy minden funkcióhoz illetve feladathoz csak a feladat ellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.

e) A hozzáférés-védelemre vonatkozó szabályoknak tartalmazniuk kell a jelszó-hossz és bonyolultság meghatározását, az időszakos jelszócsere szabályozását, a felhasználók kitiltási előírásait, illetve a hozzáférés-védelmi eszközök gyártásának, tárolásának, szétosztásának, használatának és kivonásának előírásait.

f) Az alapjogosultsági szint mindenkit megillet, aki az intézménnyel munkavállalói vagy tanulói jogviszonyban áll, és aláírásával igazolta, hogy az IBSZ tartalmát megismerte, annak betartását vállalja. Az alapjogosultsági szint adható (pl. tanfolyam esetén) az intézménnyel jogviszonyban nem állók részére is. A további jogosultsági szinteket az alapszint kiegészítéseként kell értelmezni. Az egyedi igényeket az erre rendszeresített igénylőlapon kell kérni. A felhasználótól a jogosultsági szintjének megfelelő jogot megtagadni csak indokolt esetben lehet. A jogosultsági szintnek megfelelő szabályok betartása a hálózatba nem kötött eszközök használata esetén is kötelező.

(14) A felhasználói jogosultságok szintjei:

Szint:	Jogosultak:	Jogok:
Alap	Az intézmény bármely tanára vagy tanulója	Egyéni azonosító, Internet használat, saját könyvtár a szerveren
Titkársági	Titkársági dolgozók	Alap + hozzáférés a tanulmányi ügyekkel kapcsolatos dokumentumokhoz
Gazdasági	A gazdasági osztály dolgozói	Alap + hozzáférés a gazdálkodással és a dolgozókkal kapcsolatos rendszerekhez
Operátor	Az adott feladatra kijelölt személy	Speciális jogok a kiadott feladatok ellátásához
Rendszergazda	A központi rendszerek rendszergazdái	Korlátlan jog az adott központi rendszerhez

1.3. Személyekkel kapcsolatos biztonság

(1) Az IBSZ szerinti információbiztonsági irányelveknek meg kell jelenniük a munkaköri leírásokban. A munkaköri leírások biztonsággal kapcsolatos részeinek kidolgozása során mérlegelni kell az adott munkatárs érintettségét.

(2) Minden dolgozónak titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik, hogy a munkája, tevékenysége során tudomására jutott, az intézmény számára értéket jelentő információt sem munkaviszonya fennállása idején, sem annak megszűnése után nem hozza harmadik fél tudomására.

(3) Amennyiben a felhasználók bármilyen biztonsági incidenssel, biztonsági hiányossággal kapcsolatos szoftver, illetve hardver-hibára utaló jelet tapasztalnak, azt haladéktalanul jelenteniük kell a rendszergazdáknak.

(4) A felhasználó azonosítása – hitelesítése – minden informatikai rendszer biztonságának alapja. Az intézmény informatikai szolgáltatásait különböző szintű, a veszélyeztetettséggel és az általa kezelt adatok érzékenységével arányos hitelesítési rendszerrel kell ellátni. A felhasználói neveket és jelszavakat az ügyfél és a szolgáltatást nyújtó szerver között titkosítva kell továbbítani. Ennek technikai feltételeit a rendszergazdák biztosítják. Az intézmény dolgozói – belépésükkel egy időben – felhasználói azonosítót szereznek a központi szolgáltatásokhoz. Ezzel a felhasználói azonosítóval a dolgozó az alapjogok birtokosa lesz, vagyis használhatja az intézmény hálózatát, eléri az Internetet, levelezni tud a központi levelező szerveren, és lehetővé válik számára az oktatáshoz, munkához szükséges adatok elérése. Az iskola tanulója a beiratkozáskor ill. az első informatika órán megkapja felhasználónevét és jelszavát, amellyel tanulmányai befejezéséig rendelkezik a számára szükséges alapjogokkal. Az alapjogok birtokosa jelszavát saját elhatározásból korlátozás nélkül cserélheti.

(5) A rendszergazdák az alapjogokon felül, üzemeltetési feladataiknak megfelelően többletjogokkal rendelkeznek. Az intézmény központi szolgáltatásait biztosító szerverekhez egyedi azonosítóval férhetnek hozzá, amelyeket a rendszer naplóz. A központi szolgáltatásokat végző szerverek adminisztrátori jelszavait zárt borítékban, páncélkazettában kell őrizni. A páncélkazettához csak az igazgatónak lehet kulcsa.

1.4. Eszközökkel kapcsolatos biztonság

(1) Az eszközök elhelyezésénél figyelembe kell venni a biztonsági követelményeket, törekedni kell arra, hogy a természeti hatásokból, a fizikai környezet változásaiból eredő kockázatok minimálisak legyenek. Megfelelő fizikai környezet megakadályozza a jogosulatlan hozzáférést is az informatikai eszközökhöz.

(2) Az eszközöket a strukturált hálózat szabályainak és a helyi sajátosságok figyelembe vett adottságainak megfelelően kell elhelyezni. Fokozottan védett adatokkal dolgozó rendszerek elhelyezésére különös figyelmet kell fordítani.

(3) A különböző fizikai, környezeti hatások, egyéb események, amelyek az intézmény informatikai rendszerére hatással lehetnek:

a) lopás,
b) tűz,
c) robbanás,
d) füst,
e) vízbetörés,
f) áramellátás zavara, megszakadása,
g) por, szennyeződés,
h) telephelyek közelében végzett földmunkák,
i) természeti katasztrófa.

(4) Az informatikai eszközöket védeni kell az áramellátás zavaraiból, megszakadásából származó, biztonsági problémát okozó működés ellen. Az alkalmazott áramellátás kialakításánál tekintetbe kell venni az eszköz gyártójának előírásait, a szükséges rendelkezésre állás mértékét és az anyagi lehetőségeket.

(5) Az informatikai eszközöket a gyártó által előírt környezeti paramétereket biztosító helyiségben kell elhelyezni, ennek érdekében a védett helyiségekben légkondicionáló berendezéssel biztosítani kell az előírt hőmérsékletet és páratartalmat.

(6) A strukturált kábelezés biztosítja, hogy az intézményben, a telekommunikációs és áramellátó vezetékezést külön tálcában, egymástól elválasztottan vezessék. A nem strukturált hálózatok építésekor, javításakor figyelemmel kell lenni, hogy lehetőleg a szétválasztás megtörténjen. A kábeleket csatornán kívül vezetni – még ideiglenes megoldásként – sem szabad.

(7) A számítógépes hálózat végződéseit az aktív hálózati elemeken adminisztrálni kell, a használaton kívüli végződések esetében az aktív eszközökön szoftveres vagy egyéb módon biztosítani kell, hogy illetéktelenek ne férhessenek hozzá.

(8) A biztonsági követelmények (rendelkezésre állás, sértetlenség) teljesítése érdekében az eszközök rendszeres karbantartásáról gondoskodni kell.

a) A gyártó ajánlásainak figyelembe vételével, illetve a szoftver frissítés szempontjainak figyelembevételével kell a karbantartást végezni.
b) A karbantartást és a szükséges javítási munkákat csak arra felhatalmazott személy végezheti.
c) Az ütemezett karbantartási munkákat előzetesen be kell jelenteni, amennyiben a karbantartás idejére szolgáltatás kimaradása várható,
d) A hibákat és rendszerleállásokat és a tervezett karbantartási munkákat dokumentálni kell.

(9) A személyes használatban lévő munkaállomások, hordozható számítógépek karbantartását – ha ehhez a szükséges ismeretek birtokában van – a felhasználó végzi, vagy a karbantartással megbízott informatikai szaktudással rendelkező dolgozó. Az adathordozón tárolt adatok biztonságáért minden esetben a felhasználó felel.

(10)Otthoni munkavégzés során is be kell tartani a biztonsági szabályokat. A távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó a hálózaton titkosított formában haladjon, amennyiben ez lehetséges, az adatforgalmat is titkosítani kell.

1.5.Az üzemeltetés biztonsági normái

(1) Az intézmény informatikai infrastruktúrájának és központi szolgáltatásainak üzemeltetését részben papíron, részben elektronikus formában dokumentálni kell. A dokumentálásnak ki kell terjednie:

a) a konfigurációkezelésre,
b) az ügyeleti rendszer biztosítására,
c) a telefonszámok, elérhetőségek nyilvántartására, váratlan események kezelésére,
d) a rendszerleállások, újraindítások kezelésére,
e) a külső üzemeltetőkkel történő kapcsolattartásra.

(2) Kapacitás felügyelet: az informatikai eszközök kapacitását folyamatosan felügyelni kell. A jövőbeli kapacitásigényeket a jelenlegi helyzetnek és az elvárásoknak megfelelően kell megtervezni. Valamennyi központi szolgáltatás igénybe vételekor a felhasználó tudomására kell hozni, hogy a közös tárolókapacitásokból mekkora rész jut rá, és tájékoztatni kell arról is, hogy kapacitáshiány esetén miképpen tud helyet felszabadítani. Külön kérésre a rendszergazdák többletkapacitást biztosíthatnak a munka folytatásához.

(3) Javítások, frissítések: a rendszerek javítása, frissítése kiemelten fontos feladat, melyet a rendszergazdák végeznek el.

(4) Vírusvédelem: meg kell tenni minden lehetséges intézkedést a veszélyes programok által okozott incidensek kiküszöbölésére. Ennek érdekében – szükség szerint – hatékony vírusellenőrző alkalmazásokat kell telepíteni mind a munkaállomásokra, mind pedig a szerverekre és határvédelmi eszközökre.

a) A felhasználóknak be kell tartaniuk a vírusvédelemre vonatkozó elemi szabályokat és az ide vonatkozó egyéb rendelkezéseket. Tisztában kell lenniük azzal, hogy vírusfertőzést kapni csak az egyik biztonsági kockázat. Előfordulhat, hogy a felhasználó maga válik vírusgazdává, ezzel veszélyeztetve a környezetében dolgozó munkatársait és a hálózat többi felhasználóját is, továbbá, kikerülve az Internetre, ismeretlen felhasználókat is.
b) Az intézmény központi rendszereit külön vírusszűrő szoftverek védik. A rendszergazdák feladata, hogy a védelmi szoftverek a központi rendszereken automatikusan frissüljenek. A munkahelyi munkaállomáson a rendszergazdák által javasolt vírusvédelmi rendszert célszerű használni, hogy az automatikus frissítési szolgáltatását igénybe lehessen venni.
c) A rendszergazdáknak tájékoztatnia kell a felhasználókat a vírusok felbukkanásáról, a velük szemben követendő magatartásról, illetve az időnként terjedő hamis vírusfenyegetettségről.
d) A felhasználónak tilos lánclevelet, hamis vírusriasztásokat küldeniük a központi levelező rendszeren keresztül.
e) Vírusfertőzésről, mint biztonsági incidensről, a rendszergazdákat értesíteni kell abban az esetben is, ha a vírus terjedését sikerült helyben megakadályozni.

(5) Kéretlen levelek, reklámok szűrése (spam): a kéretlen levelek központi szűréséről a rendszergazdák üzemeltetésében álló szerverek gondoskodnak. A levelek kéretlennek minősítése egy folyamatos valószínűségi skálán történik, amely a leveleket – pontszám alapján – három csoportba sorolja:

a) nem gyanús: változatlanul továbbítjuk a címzettnek,
b) gyanús: megjelölve továbbítjuk a címzettnek,
c) nagy biztonsággal spam: karanténba kerülnek, és a címzett tájékoztatást kap a visszatartott levélről, amelyet a karanténban megtekinthet. A levél egy hónap múlva törlődik.

(6) Külső és belső támadások kockázatainak csökkentése érdekében központi tűzfal-üzemeltetés javasolt. Esetleges támadásokat a rendszergazdáknak kell jelezni.

1.6. Hálózat menedzsment

Az intézmény belső hálózatán (Intranet) használt központi szolgáltatások kliens-szerver alapúak, amelyek nagymértékben függenek a hálózat működési paramétereitől, ezért a hálózat védelme és folyamatos működése, valamint annak felügyelete az intézmény alapvető érdeke.

Az Intranet ellenőrzése során végzendő feladatok:

a) a hálózat működőképességének folyamatos felügyelete és a meghibásodás naplózása,
b) a hálózat meghibásodása esetén a hibaelhárítás haladéktalan megkezdése, különösen problémás esetben akár az aktuális iskolai munkafolyamatot megszakítva,
c) aktív hálózati elem meghibásodása esetén a csereeszközről való gondoskodás,
d) folyamatos statisztika készítése a forgalmi adatokról.

Határvédelmi eszközök üzemeltetése: az intézmény belső hálózatát az Internettől tűzfal funkciójú eszközök választják el. A tűzfalak szabályrendszereinek kialakítása, a tűzfalak beállításainak folyamatos karbantartása, a naplók elemzése, a szükséges intézkedések megtétele a rendszergazdák feladata.

(1) Biztonsági mentések

Az üzembiztonság fenntartása, az adatok védelme érdekében a központi informatikai szolgáltatásokat ellátó rendszerek biztonsági mentéséről a rendszergazdáknak folyamatosan gondoskodnia kell. A biztonsági mentésnek ki kell terjednie az alábbi aktív vagy szerver feladatokat ellátó eszközökre:

e) hálózati switch-ek, routerek és vezeték nélküli hozzáférési pontok (aktív eszközök),
f) tűzfal szabálylistája,
g) névkiszolgálók adatbázisa (DNS),

h) központi címtár,
i) központi levelezés,
j) intézményi weboldal, és médiafelületek,
k) központi szoftverek.

(2) A biztonsági mentések adathordozóit az adatok keletkezési helyétől eltérő helyen kell tárolni, amiről az Adatkezelési Szabályzat rendelkezik.

(3) A mentések végrehajtásának menete: a biztonsági mentések során olyan eljárást kell alkalmazni, amely egyértelműen biztosítja, hogy a tároló médiára az adatok sértetlenül és visszaolvashatóan felírásra kerüljenek.

(4) A központi szervereken tárolt adatok (címtár, intézményi levelező rendszer, intézmény weboldal, intézményi médiadelületek-, médiamegjelentetések, felhasználói home könyvtárakban tárolt adatok) biztonsági mentéséről a rendszergazdák kötelesek gondoskodni.

(5) A gazdasági irodában, titkárságon és a könyvtárban helyileg telepített nyilvántartó- és könyvelő programok napi mentéséről az adott szoftver felhasználója köteles gondoskodni.

1.8 Vezeték nélküli hálózat (WiFi) használata

Az iskolában üzemeltetett vezeték nélküli hálózathoz az arra jogosult személyek kaphatnak hozzáférést, minden felhasználó egyedi névvel és jelszóval történő azonosítása után. A felhasználók a saját csatlakozási adataikat harmadik félnek nem adhatják ki, abba az esetben a felhasználóval szemben szankciókra kerül sor.

a) **Eduroam WiFi:** a KIFÜ által üzemeltett vezeték nélküli hálózat, melynek használatához jogosult személyek az iskola tanulói, tanárai, dolgozói, amihez a szükséges egyéni azonosítót és jelszót személyesen kapja meg minden felhasználó, mely az üzemeltető (KIFÜ) szabályzatának megfelelően nem osztható meg: csak az adott személy jogosult használni. Minden felhasználó saját maga végezheti és végzi el a csatlakozást. Egyes iskolai eszközök – tanítási órákon, foglalkozásokon használt notebookok, tabletek, stb. – szintén WiFi kapcsolatot igényelnek, amelyekhez a szükséges beállításokat a rendszergazda végzi el, és amely hozzáférési adatokhoz kizárólagos jogosultsága van.
b) **Guest WiFi:** a KIFÜ által üzemeltetett vezetéknélküli hálózat, melynek használatához jogosult személyek azon iskolán kívüli személyek, akik valamilyen iskolai rendezvényt látogatnak meg, és a rendezvény idejére WiFi hozzáférést kérnek. A csatlakozáshoz szükséges azonosítót és jelszót a titkárságon ill. a rendszergazdától igényelhetik, amely időszakonként – technikai és biztonsági okokból – változik.
c) **ZayKoli WiFi:** az iskola által üzemeltett vezeték nélküli hálózat, melynek használatához jogosult személyek a kollégiumban elszállásolt tanulók és kollégiumi nevelők, amelyhez szükséges közös azonosító és jelszó elérhető a kollégiumi nevelők és a rendszergazda által.

1.9 Elektronikus levelezéssel kapcsolatos biztonsági szabályok

- Az elektronikus levelezési szolgáltatás használata során az alábbi szabályokat kell betartani:
- A felhasználó nem titkolja el személyazonosságát az Internet-használat közben.
- A felhasználó tudomásul veszi, hogy a központi levelezés során a felhasználó levelezési forgalma naplózásra kerül.
- A levelezési szolgáltatás mind a munkatársak közötti, mind az intézményen kívüli munkaköri kapcsolattartásra felhasználható.
- Az elektronikus levélhez fájl csatolható, amelynek mérete korlátozott.
- Az elektronikus levélhez csatolt fájl nem lehet futtatható állomány, nem lehet tömörített csomagban futtatható állomány, nem lehet továbbított reklám.

- A felhasználó tudomásul veszi, hogy az e-mail cím kötött, és nem változtathatja meg.
- A levelezési rendszeren tilos biztonsági szempontból érzékeny anyagot illetéktelen személy részére hozzáférhetővé tenni.
- Tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes, illetve üzleti érdekeit sértheti.
- Az elektronikus levelezési jogosultsággal rendelkező felhasználó csak saját nevében küldhet levelet, kivéve, ha erre felelős vezető utasítja.
- Tilos rasszista, szemérmet és jó ízlést sértő, valamint szélsőséges politikai nézeteket képviselő tartalmú levelet küldeni.
- A szellemi tulajdon védelme az Internetre is kiterjed.

1.10 Az Internet használattal kapcsolatos szabályok

Az intézmény belső hálózatába működő munkaállomások alaphelyzetben Internet eléréssel rendelkeznek. Az Internetet használata során az Intézmény fenntartja a jogot arra, hogy a felhasználók Internet forgalmát, tartalmát figyelemmel kísérje, és naplózza. A felhasználónak tisztában kell lennie azzal, hogy az Internet használata biztonsági kockázattal jár, ami nem csak a személyes használatában lévő munkaállomást veszélyeztetheti, hanem a hálózat egyéb eszközeit is. A felhasználónak tisztában kell lennie azzal is, hogy nem használhatja az Internet elérését törvények és szabályok tudatos vagy szándékos megsértésére. Az Internetről letöltött szoftver vagy fájl jogtisztaságáért az intézmény, mint jogi személy felel, ezért fenntartja jogot, hogy a szabályok megsértőivel szemben szankciókat alkalmazzon. Illegális tevékenység céljára használt Internet elérés fegyelmi eljárást eredményezhet.

Hozzáférés ellenőrzése:

A felhasználók regisztrálása: az intézmény dolgozóinak többsége napi munkája során hálózatba kötött munkaállomáson végzi feladatait. Ezért a munkaállomásokon központosított felhasználó regisztrálás nem történik. Minden személyes használatban lévő munkaállomáson szabadon választható a felhasználó azonosítása.

A központi szolgáltatások esetében a regisztráció kötelező, és a feladatok függvényében jogosultságok hierarchiája valósul meg. Minden felhasználó csak annyi jogot kap, amennyi a feladata elvégzéséhez szükséges. Különösen védett adatok esetében a személyes regisztráción felül a titkosított csatorna használatához is szükséges azonosítót alkalmazni.

A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie, a kezdeti jelszót a felhasználó köteles az első használat során megváltoztatni. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:

- Tilos könnyen kitalálható jelszavakat választani!
- Tilos a felhasználónevet jelszóként használni!
- Tilos a vezetéknevet és a keresztnevet jelszóként használni!
- Tilos azonos számokból, vagy betűkből jelszót használni!
- Tilos a jelszót nyilvános helyen kiírva tartani (például: monitorra ragasztva)!
- Ajánlott a számok és betűk keverése jelszavak használatakor.
- Ajánlott a kis és nagybetűk keverése jelszavak használatakor.
- Intézményi jelszót a felhasználó intézményen kívüli rendszerekben nem használhat.

Rendszergazda a szervereket védetlenül nem hagyhatja magára, és a feladata elvégzése után ki kell jelentkeznie a rendszerből, vagy zárolnia kell azt.

1.11 Rendszerhasználat felügyelete (monitoring)

A naplózást az intézmény minden központi szolgáltatást futtató eszközén, valamint a határvédelmi eszközökön alaphelyzetben engedélyezni kell. A szerverek, hálózati eszközök, valamint a biztonsági rendszer elemeinek naplóállományait rendszeresen ellenőrizni kell, és a biztonsági megfontolásokat figyelembe véve meghatározott ideig tartó tárolásáról gondoskodni kell.

A naplózás során rögzítenie kell:

- a rendszer leállását és újraindulását,
- a rendszerben fellépő hibákat,
- felhasználó bejelentkezését, vagy sikertelen bejelentkezési kísérleteket,
- tranzakció végrehajtását,
- új felhasználó felvételét, törlését.

Az intézmény informatikai rendszereinek esetleges hosszabb idejű működésképtelensége esetén mindent meg kell tenni a rendszer minél gyorsabb helyreállítása, és a folyamatos üzemmenet biztosítás érdekében. Katasztrófa, vagy kritikus helyzet minél gyorsabb megoldása érdekében, a rendszergazdák igazgatói engedéllyel bármikor, vagyis akár a lezárt épületbe is bejuthatnak. Ez vonatkozik a munkaszüneti napokra, ünnepekre, és a munkaidőn kívüli időre (éjszaka) is.

A szabályzat megsértésének gyanúja esetén az esetet ki kell vizsgálni, és a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket.

A szabályzat elkészülte és bevezetése után gondoskodni kell annak évenkénti felülvizsgálatáról, a változásokat követő módosításáról.

Nyíregyháza, 2023. szeptember 1.

Vargáné Nemes Ildikó
igazgató

Asztalos Szilárd
rendszergazda

Nyíregyházi SZC Zay Anna Technikum és Kollégium Nyíregyháza 1