Informatikai Biztonsági Szabályzat

I. Bevezetés

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) tartalmazza az informatikai rendszerrel kapcsolatos védelmi intézkedéseket.
Az IBSZ következetes végrehajtása biztosítja az informatikai rendszer zárt, teljes körű, folyamatos védelmét és szabályozásán keresztül lehetővé teszi, hogy a rendszer által kezelt adatok bizalmassága, sérthetetlensége, hitelessége, működőképessége, illetve rendelkezésre állása megvalósuljon. A védelmi intézkedések felölelik a fizikai és ügyviteli védelmet is.
Az IBSZ kidolgozásáért és karbantartásáért a Jegyző a felelős.

II. Az IBSZ hatálya

1. Szervezeti hatály

Az IBSZ hatálya:
Zalacsányi Közös Önkormányzati Hivatal

- A költségvetési szerv székhelye: 8782 Zalacsány, Zrínyi Miklós u. 6.
- A költségvetési szerv - kirendeltsége: 8395 Felsőpáhok, Szent István u. 67.
- A költségvetési szerv - kirendeltsége: 8371 Nemesbük, Petőfi S. u. 1.

(továbbiakban együttesen Hivatal)

2. Személyi hatály

Az IBSZ személyi hatálya: a Hivatal valamennyi vezetője, ügyintézője, az informatikai rendszerek felhasználói, fejlesztői és üzemeltetői.
Ezeken kívül a dokumentum hatálya kiterjed a Hivatallal külső, megbízásos (szerződéses) eset munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a munkavégzésre vonatkozó szerződésekben kell biztosítani.

3. Tárgyi hatály

Az IBSZ tárgyi hatálya: A Hivatalban alkalmazott valamennyi informatikai rendszer, amely rögzíti, feldolgozza, tárolja, felhasználja, illetve felügyeli és ellenőrzi a Hivatalnál keletkező, valamint feldolgozott adatokat és információkat.

III. Értelmező rendelkezések

Az IBSZ-ban használt szakkifejezések jelentése a mindenkor hatályos 2013. évi L. törvény I. fejezet 1. pontjában található.

IV. Eljárási szabályok

1. Biztonsági célkitűzések

Az IBSZ tárgyi hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

2. Kockázatelemzés és –kezelés

A szervezet megfogalmazza és dokumentálja, valamint kihirdeti a kockázatelemzési és kockázatkezelési eljárásrendet, mely a kockázatelemzési és kockázatkezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő.

3. Biztonsági osztályba sorolás

Az IBSZ tárgyi hatálya alá tartozó elektronikus információs rendszer biztonsági szintje 2013. évi L. törvény 9.§ alapján: **2. (azaz kettes)**

4. Biztonsági szintek

A Hivatal egyes számítógépei, informatikai eszközei, valamint a rajtuk futtatott alkalmazások különböző jelentőséggel bírnak rendszer biztonságos működésének szempontjából. A tevékenységek biztonsági kockázatának figyelembe vételével a következő szintek kerültek kialakításra:

I. szint:

A funkció és biztonság szempontjából legfontosabb eszközök és berendezések. Közös jellemzőjük, hogy még rövid időre (2-4 óra) történő leállásuk sem viselhető el a rendszer számára, illetve hiányuk és a rajtuk tárolt adatok bizalmasságának, sérthetetlenségének és hitelességének elvesztése olyan biztonsági problémákat okoz, amelynek kockázata nem vállalható.

II. szint:

Azon eszközök és berendezések, melyek működésének viszonylag rövid ideig (1-2 napig) tartó kiesése elviselhető terhet ró a Hivatalra, mind a tevékenység ellátása, mind a biztonság szempontjából. A rajtuk tárolt adatok bizalmassága, sérthetetlensége nem éri el az I. szint leírásánál meghatározott biztonsági fokozatot.

III. szint:

Azon eszközök és berendezések, melyek működésének még hosszabb ideig (1 hét) tartó kiesése sem befolyásolja jelentős mértékben a Hivatal működését.

Az informatikai infrastruktúra és eszköz park minden elemét be kell sorolni valamelyik szintre annak megfelelően, hogy működésének megszűnése hogyan hat a Hivatal egészének funkcionalitására.

A besorolás a Jegyző feladata.

A három kategóriába tartozó eszközökre csoportonként és eszköztípusonként más-más biztonsági előírások vonatkoznak.

5. Védelmi intézkedések a biztonsági célkitűzések alapján

A Hivatal területén bevezetett informatikai védelmi biztonsági intézkedések csökkentik az intézmény területén fellépő károk bekövetkezésének valószínűségét.

A védelmi intézkedések kötelező jellegűek a Hivatal munkavállalóira és az IBSZ hatályában meghatározottakra nézve. A védelemi intézkedésektől eltérni csak egyedi esetben, a Jegyző jóváhagyásával lehet.

Az IBSZ-ben foglaltak betartásáért mindazon személyek kötelezettek és felelősek, akikre az IBSZ hatálya kiterjed, betartásáért a Jegyző felelős. Ennek érdekében a belépő új munkatársnak a próbaidő alatt számot kell adnia az IBSZ és kapcsolódó dokumentumainak olyan szintű ismeretéről, mely alkalmassá teszi őt a megfelelően biztonságos munkavégzésre.

5.1 Fizikai védelem és fizikai környezet védelme

Figyelemmel kell lenni a más jogszabályban meghatározott tűz- és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre.

Biztosítani kell, hogy a Hivatal fizikailag folyamatosan védett környezetben legyenek mind a hivatali nyitvatartási időn belük, mind azon kívül.

Az állandó belépésre jogosultakról és a részükre kiadott, az épületbe bejutást biztosító kulcsokról nyilvántartást kell vezetni, hasonlóan az ideiglenes belépésre kíséret nélkül jogosultakról is, valamint naplózni kell azokat. A nyilvántartás aktualizálásáért a Jegyző a felelős.

A riasztási eseményekről feljegyzést kell készíteni.

5.2 Fizikai hozzáférés és üzembiztonság

Az I. és a II. szintbe sorolt számítógépek jelentősége – különös tekintettel a rajtuk futó rendszerekre és az általuk tárolt adatokra – nagy mértékben meghaladják a III. szintbe sorolt informatikai eszközök jelentőségét, ezért biztonsági szempontból kiemelten kezelendők. Az I. és a II. szinten elhelyezkedő eszközökre az alábbi rendelkezéseket kell betartani:

5.2.1 Számítógépek (I. és II. szint)

A számítógépeket zárható helyiségekben kell elhelyezni és üzemeltetni. A helyiségekben csak a jogosultsággal rendelkezők tartózkodhatnak. A jogosultsággal nem rendelkezők kizárólag a Hivatal **vezetője** vagy ügyintézője kíséretében tartózkodhatnak.

A számítógépek üzemeltetésére kijelölt helyiségek kialakításánál a következő minimális követelményeknek kell eleget tenni:

a) A nyílászárókat biztonságosan le kell zárni. Az alkalmazott lezárási technológiáknak a behatolás-védelmi szempontokat és „vis major" helyzeteket figyelembe kell venni.
b) Váratlan áramkimaradás esetére a számítógépeket szünetmentes áramellátást biztosító eszközökkel kell ellátni.
c) Az elektromos hálózatban fellépő anomáliák ellen a Hivatal helyiségeiben megfelelő védelmet kell kialakítani (villámvédelem, feszültség-ingadozás, feszültség csúcsok, stb.)

5.2.2 Hálózati eszközök

A hálózat technikai védelmét tűzfalrendszerrel kell biztosítani, mely képes kontrollálni a bejövő és a kimenő internetes forgalmat. A hálózat humán oldali védelme során ki kell dolgozni a felhasználóktól elvárt internetes magatartási mintákat, aminek ki kell terjednie az engedélyezett tevékenységekre, a tiltott tevékenységekre és az incidens észleléskori teendőkre egyaránt.

A Hivatal védelmének szempontjából az I. és a II. szintbe sorolt hálózati eszközök esetében az alábbi rendelkezéseket kell betartani:

a) Az eszközöket fizikai behatástól védett helyen kell tárolni és amelyik eszköznél lehetséges, azt külön zárható helyen kell elhelyezni.

5.2.3 Számítógépek, munkaállomások

Az egyedi felhasználású számítógépek esetében és a munkaállomásként üzemelő, hálózatra kapcsolt számítógépek fizikai hozzáférésénél az alábbi intézkedéseket kell betartani:

a) A munkaállomásokat csak zárható helyiségekben szabad tárolni. Amikor a helyiségben nem tartózkodik senki, az ajtót zárva kell tartani.
b) Az állandó felügyelet nélküli helyiségekben csak olyan számítógépek és munkaállomások telepíthetők, amelyek az operációs rendszeren és futtatandó programokon kívül semmilyen adatot nem tartalmaznak és csak a használatuk időtartama alatt lehet hálózatba kötve.
c) A számítógépek és a munkaállomások telepítésénél gondoskodni kell a lehető legbiztonságosabb – rázkódás-, zuhanásmentes – elhelyezésről.

5.2.4 Leltárkészítés

A Hivatal minden vagyonelemét leltárba kell venni. Tekintettel arra, hogy az informatikai célú leltározási eljárás különbözik a könyvelési és gazdasági célú leltározási eljárásoktól, biztosítani kell a két leltár közötti konzisztencia fennmaradását.

A konfigurációkat legalább az alábbi kategóriákra kell bontani:

1. Hardveres eszközök
    a) szerverek
    b) munkaállomások (asztali és hordozható)
    c) mobil eszközök (tablet, okostelefon)
    d) hálózati elemek (router, switch, hub, kábelezés)
2. Szoftveres elemek
    a) operációs rendszerek (számítógép, mobil, firmware)
    b) alkalmazások (helyi és távoli kliensek, adatbázis-kezelők, middlewarek)
    c) eszközök konfigurációs állományai (beállításai)

5.2.5 Egyéb üzembiztonsági intézkedések

5.2.5.1 Általános intézkedések:

a) Az informatikai eszközöknek funkcionálisan megfelelő hardver tartalékkal kell rendelkezni.

b) Gondoskodni kell az informatikai eszközpark minden elemének (hardver és szoftver eszközök esetében egyaránt) folyamatos karbantartásáról.
c) A hardver eszközök beszerzésénél a megbízható referenciákkal nem rendelkező termékektől el kell zárkózni.
d) Meghibásodás esetén, ha a hiba természeténél fogva külső cég beavatkozását igényli, a cégnek biztosítania kell a Hivatal feladatellátásának folyamatosságához szükséges feltételeket.

5.2.5.2 A számítógépek és a munkaállomások esetében az alábbi intézkedéseket kell betartani:

a) A felhasználó semmilyen hardver elemet a munkahelyi számítógépébe nem telepíthet, és abból el nem távolíthat.
b) A napi munka befejeztével a felhasználónak mindig ki kell lépnie az alkalmazott programokból, a hálózat másik számítógépén futtatott alkalmazásból és az operációs rendszerből is. Ezt követően ki kell kapcsolnia az általa használt informatikai eszközöket.
c) A felhasználó a számítógépet csak rendeltetésének megfelelően használhatja.
d) Az asztali számítógépek és egyéb informatikai eszközök a Hivatalból történő elvitele minden felhasználó számára szigorúan tilos.

5.2.5.3 A hordozható számítógépek használatára az alábbi rendelkezések vonatkoznak:

a) Hordozható számítógép használatát a jegyző engedélyezi.
b) A használó a részére átadott hordozható számítógép biztonságos szállításáról és tárolásáról. Biztosítania kell az illetéktelen hozzáférés megakadályozását.
c) Nyilvános helyen szigorúan tilos a Hivatallal kapcsolatos bizalmas adatokat, információkat tartalmazó hordozható számítógépek felügyelet nélkül hagyása!

5.2.6 Szoftver eszközök (licencek)

A szoftver licencekről és egyéb, a szoftverek használatához kapcsolódó jogosultságokról (pl. internetes adatbázis hozzáférések, stb.) összesített nyilvántartást kell vezetni. A nyilvántartás vezetését a Jegyző által megbízott személy végzi.

A nyilvántartásnak ki kell terjednie a számítógépeken és a hálózati eszközökön futó szoftverekre, a szoftverekhez kapcsolódó egyéb felhasználói jogosultságokra és minden alkalmazásra, valamint azok kiegészítésére is. A nyilvántartásnak tartalmaznia kell a licenc jogosultság pontos megnevezését, mennyiségét és időintervallumát is. A nyilvántartásnak biztosítania kell, hogy a meglévő licenc keretek felhasználásának pillanatnyi állapotát is mutassa.

A Hivatal tulajdonában lévő szoftvereket és adatokat tartalmazó adathordozók kivitele a Hivatal területéről kizárólag munkavégzés és hivatali adatszolgáltatási-, és bemutató feladatok ellátása célból megengedett.

A számítógépeken és a hálózati eszközök futtatott rendszerek programjainak, adatbázisainak és konfigurációs állományainak teljes vagy részleges másolatai, mentései, exportjai, továbbá a munkavégzéshez nem szükséges adat vagy szoftver nem másolható, nem telepíthető, azon a munkaidőn túl nem tárolható, kivéve, amelyet a jegyző írásban engedélyezett.

A számítógépekre szoftver és adatbázis telepítését csak a jegyző által megbízott személy végezheti.

A II. szintbe sorolt számítógépeknek és munkaállomásoknak, valamint a bizalmas adatokat feldolgozó személyi számítógépeknek olyan operációs rendszerrel kell rendelkezniük, amelyek képesek az adatok, információk védelmére, továbbá olyan fájlrendszer használatára, amelyben a könyvtárakra és fájlokra a hozzáférési jogosultsági rendszer beállítható. Ezeken a számítógépeken az ilyen fájlrendszer használat kötelező.

5.2.7 Vírusvédelem

A számítógépek vírusvédelmére kiemelten az alábbi rendelkezéseket kell betartani.

a) Minden munkaállomásra vírusellenőrző szoftvert kötelező telepíteni.
b) A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetében meg kell vizsgálnia az adathordozó tartalmát, és amennyiben vírust talált, nem engedhet másolást, futtatást a vírusok leirtásának megoldásáig.
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 a vírusellenőrző szoftver beállításainak módosítása tilos!
e) Vírus felbukkanása esetén a szoftver kísérelje meg azt kiirtani.
f) A kárt okozó, illetve a rendszerek működését befolyásoló vírusfertőzés esetén haladéktalanul meg kell kezdeni a hatástalanítást.
g) A hatástalanítást a Jegyző által megbízott személy végzi.

Az elektronikus információs rendszert védeni kell a kártékony kódok ellen, fel kell deríti és megsemmisíteni azokat. A védelmi mechanizmusokat frissíteni kell a hatékonyság érdekében, az információs rendszeren rendszeres ellenőrzéseket kell végrehajtani.
Az elektronikus információs rendszer felügyeletét biztosítani kell!
Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

5.2.8 Rendszer és kommunikációvédelem

Ellenőrizni és védeni kell a szervezetből kilépő és az oda belépő információkat.
A Hivatal előállítja és kezeli a kriptográfiai kulcsokat, a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.
Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.
Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

5.2.9 Mentések

Az informatikában a legnagyobb értéket a számítógépeken tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.
A mentés célja:

a) A ritkán használt, illetve a kulcsfontosságú adatok rendszerezett, biztonságos és visszakeresésre alkalmas tárolása
b) Az előre nem látott adatsérülés, vagy adatvesztés esetén az adatok a – korábban szabályozott módon eltárolt – mentésekből hiánytalanul visszaállíthatóak legyenek.

Mentés során a visszaállításhoz szükséges valamennyi adatot és beállítást is tárolni kell.

Az adatok az I. és II. szintbe sorolt számítógépeken kell tárolni, mentést a III. szintű munkaállomásokról nem kötelező központilag készíteni.

Az I. és II. szintű számítógépeken található adatállományok mentésénél az alábbi rendelkezéseket kell betartani:

a) A számítógépek mentéseit havonta, vagy szükség esetén kell végrehajtani.
b) A mentésből a teljes adatállománynak, az adatokat futtató szoftvernek és a szoftverkörnyezet beállításainak is visszaállíthatónak kell lennie.
c) A mentéseket elkülönítve, biztonságosan zárható helyen kell őrizni.
d) A mentett adatokhoz csak az arra jogosultak férhetnek hozzá. A jogosultságokat a jegyző szabályozza.
e) A mentések elkészítéséért és az esetleges visszaállításokért felelősöknek a munkavégzésüket biztosítandóan megfelelő jogokkal kell rendelkezniük.

A hálózatba kötött III. szintű munkaállomásokon tárolt adatok megőrzésének és biztosításának érdekében az alábbi rendelkezéseket kell betartani:
Semmilyen, a Hivatal ügyvitele szempontjából fontos-, minősített- vagy személyes adatot tartalmazó fájlt nem szabad az adott munkaállomáson tárolni. Amennyiben erre szükség van, akkor a számítógép szintbesorolását meg kell változtatni.

5.2.10 Archiválási szabályok

A Hivatalban az archiválásoknak a belső utasításokban és jogszabályi rendelkezésekben foglaltakkal összhangban kell történni.
Az archivált anyagoknak visszakereshetőknek és értelmezhetőnek kell lennie.
Az archiválási eseményt mindig Jegyzőkönyvezni kell.
Az anyagok későbbi tárolására és kezelésére a mentés szabályai vonatkoznak.

5.2.11 Naplózás

A megbízható működéssel kapcsolatos eseményekről gépi, illetve manuális biztonsági naplózásokat kell végezni. Meghatározandók azok tartalmi követelményei, a naplók kezelési, értékelési és tárolási módja. A biztonsági napló tartalmi és formai követelményei legyenek összhangban az információvédelmi biztonsági naplózásnál ismertetett követelményekkel.

Belső rendszerórákat kell használni a naplóbejegyzések időbélyegeinek előállításához;

5.2.12 A logikai hozzáférések, jogosultságok

5.2.12.1 Jelszavak

Minden felhasználó jelszavát illetéktelenektől gondosan védeni kell.

A jelszavaknak az alábbi minimális kritériumoknak meg kell felelnie:

a) A számítógép bejelentkezési jelszó legalább 6 karakterből álljon, és kis- és nagybetűk, számok, valamint egyéb írásjelek közül legalább három típusút tartalmazzon.
b) Az alkalmazásokhoz tartozó jelszavak kialakítása esetében az alkalmazás által előírt módon kell eljárni.
c) A jelszó nem lehet azonos a felhasználónévvel, annak becézett formájával, vagy egyéb könnyen visszafejthető kifejezéssel.
d) A felhasználók a számítógépekbe bejelentkezve csak a munkájukhoz szükséges alkalmazásokat indíthatják el, egyéb utasításokat nem adhatnak ki.

Az a)-d) pontokban meghatározott rendelkezéseket az operációs rendszer beállításaival kell támogatni. ennek beállítását a Jegyző által megbízott személynek kell elvégezni.

A jelszavakat az egyes számítógép azonos jogosultságú használói között meg lehet osztani.

A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.

A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott vagy juthatott. Amennyiben a felhasználó meg tudja változtatni a jelszavát, a fenti esetben azt köteles a lehető legrövidebb időn belül megtenni. Ha a változtatást a felhasználó nem tudja megtenni, kérvényezni kell a Jegyzőtől.

A számítógépeket rendszergazdai jelszóval kell ellátni. A rendszergardai jelszót kizárólag a Jegyző és az általa megbízott személy ismerheti.

a) A rendszergazdai jelszót egy lezárt és aláírt borítékban a Jegyző köteles biztonságos helyen tárolni.
b) A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, illetve juthatott, vagy ha a borítékon sérülés érzékelhető.
c) A jelszót tartalmazó borítékhoz csak a jegyző és az általa írásban megbízott személy férhet hozzá.
d) A boríték csak indokolt esetben nyitható fel! A felnyitás műveletét jegyzőkönyvezni kell.

A rendszergazdai jelszóval távoli bejelentkezést csak megfelelően titkosított (ssh, ipsec) kapcsolat esetén lehet végrehajtani.

Mindenki személyesen felel a saját azonosítójával és jelszavával elkövetett illetéktelen számítógépes behatolásért, ha az azonosító és a jelszó kiszolgáltatásának oka saját gondatlansága, vagy hanyagsága volt.

A munkaviszony időleges megszűnésekor a felhasználó minden jogosultságát fel kell függeszteni. A munkaviszony végleges megszűnésekor a felhasználó minden jogosultságát és azonosítóját meg kell szüntetni. A felhasználói jogok felfüggesztéséért, illetve törléséért a jegyző a felelős.

Amennyiben a munkavállaló munkaviszonyának megszűntetésekor meg nem szüntethető azonosítóhoz tartozó jelszót ismert, a jelszót a fent leírt rendelkezések betartásával, azonnali hatállyal meg kell változtatni.

5.2.12.2 Jogosultságok

A számítógépek tekintetében a fentieken kívül az alábbi rendelkezéseket kell betartani:

a) Mivel a számítógépek nincsenek (és nem is lehetnek) fizikailag jól védhető helyen (ld. Fizikai hozzáférések és üzembiztonság), ezért védelmükről szoftveres úton is gondoskodni kell.
b) A számítógépeken futó alkalmazásokra történő belépésekhez és az Internetes adatbázisokhoz történő hozzáférésekhez kapcsolódó jogosultságokat a jegyző, az Informatikai Jogosultság Adatlapon (2. számú Melléklet) határozza meg.
c) A felhasználó az Adatlapon nyilatkozik a szoftver licencek és az internet alkalmazása feltételeinek ismeretéről és azok elfogadásáról.
d) Az Informatikai Jogosultság Adatlap a felhasználó Munkaköri Leírása mellékletét képezi, annak elválaszthatatlan és kötelező része.
e) Az Adatlap elfogadása után a Jegyző gondoskodik a jogosultságok beállításáról.
f) A már használatban lévő jogosultságok vonatkozásában a 2. számú mellékletet (Informatikai Jogosultság Adatlap) az IBSz hatályba lépését követő 30 napon belül kell a jegyzőnek kiállítani és a jogosultságok beállításáról gondoskodni.
g) A felhasználó közszolgálati jogviszonyának, munkaviszonyának megszűnésekor, annak felhasználói azonosítóját meg kell szüntetni, számítógépet át kell venni, és ezt mind az eszközökkel, mind a szoftver licencekkel kapcsolatos nyilvántartásokon át kell vezetni.
h) Ha a felhasználó munkavégzés közben elhagyja a számítógépét, képernyővédőt kell alkalmaznia.

5.2.13 Rendszer és információsértetlenség

Az információkat csak az arra jogosultak változtathatják meg és azok véletlenül sem módosulnak. Ez a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani.
Korrektek azok az információk, amelyek a valós dologi vagy feltételezett állapotot helyesen írják le.

5.2.14 Hibajavítás

A Hivatal azonosítja, jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit; telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szóba jöhető következmények szempontjából.
A Hivatal beépíti a hibajavítást a konfigurációkezelési folyamatba.

5.2.15 Rendszer és szolgáltatás beszerzés

A Hivatal elektronikus információrendszerének minden elemére kiterjedő biztonságot akkor lehet elérni, ha az információbiztonsági követelmények a rendszer teljes életciklusában érvényesíthetők, a beszerzéstől az üzemeltetésen és a fejlesztésen át a selejtezésig vagy kivezetésig. Emiatt szükség van arra, hogy az információbiztonsági felelős az életciklus minden eseménye során véleményt nyilváníthasson a tervezett módosítás biztonságra

gyakorolt hatásairól. Tekintettel arra, hogy az általános felelősség a jegyző vállain nyugszik, az információbiztonsági felelős véleményének figyelembe vételét nem lehet kötelezővé tenni, de a véleményének mellőzését csak és kizárólagosan a kockázatok tudatos felvállalásának elve alapján lehetséges megtenni.

5.3 Rendszer fejlesztés és üzemeltetés kapcsolatára vonatkozó szabályok

A Hivatal működéséhez fejlesztett alkalmazások üzemeltetésének biztonságosságára a következő pontok vonatkoznak:

a) Törekedni kell a fejlesztési, a teszt- és az éles üzemmód futtatási helyének elkülönítésére. Ennek biztosítása a Jegyző feladata.
b) Minden informatikai fejlesztési feladathoz ki kell nevezni rendszerfelelőst. A rendszerfelelős kinevezése a Jegyző feladata.
c) Külső fejlesztőknek nem lehet jogosultsága az éles alkalmazásokra.
d) Az alkalmazott szoftverek változásairól az érintett felhasználókat tájékoztatni kell, továbbá – szükség esetén – meg kell velük ismertetni a fejlesztés gyakorlati alkalmazásainak használatát és új lehetőségeit.

5.3.1 Adathordozók

A Hivatal adatforgalmazásában felhasználásra kerülő adathordozókon (floppy/CD/DVD lemez, Pendrive, stb.) történő adatátvitel esetén a következő előírásokat kell betartani:

a) A szállítás folyamán az adathordozót a sérüléstől való megóvás érdekében védő borítással kell ellátni.
b) Mágneses adathordozó esetén a védelemnek ki kell terjednie az erős mágneses tér okozta adatvesztés megelőzésére is.
c) A beérkezett (és kimenő) adathordozón első (és utolsó) lépésben mindig vírusellenőrzést kell végezni.
d) Az adathordozók szállításának biztonságáról a jegyzőnek kell gondoskodni.

A mentésre, archiválásra és bármilyen szintű elektronikus információ-tárolásra használt adathordozók esetében az alábbi intézkedéseket kell betartani:

a) Az adathordozók várható élettartamának, és a tárolt adatok/információk elévülési idejének figyelembevétele mellett meghatározott gyakorisággal felül kell vizsgálni a tárolt adatok rendelkezésre állását, illetve gondoskodni kell azok új adathordozóra történő duplikálásáról.
b) A megsemmisítésre kijelölt adathordozók fizikai megsemmisítéséről a Hivatal Iratkezelési Szabályzata vonatkozó rendelkezéseinek megfelelően kell eljárni.

A Hivatalnak meg kell határoznia az adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát.

5.3.2 Az informatikai hálózattal kapcsolatos intézkedések

A Hivatal az alább hálózatokkal rendelkezik:

a) Hivatalon belüli egységes struktúrájú LAN hálózat.
b) Internet elérés (DSL).

A belső LAN hálózatra vonatkozó biztonsági szabályok:

a) Minden, a belső hálózatra csatlakoztatott számítógépről csak azok a hálózati erőforrások érhetők el, amelyekre a felhasználónak munkája elvégzéséhez szüksége van.
b) A LAN hálózatba kapcsolat számítógépek és az Internet kapcsolat hálózati kommunikációja csak a központi routeren keresztül, ellenőrzött módon engedélyezett.

A külső hálózatok felé irányuló vonalakra vonatkozó biztonsági szabályok:

a) A Polgármesteri Hivatal külső hálózatokkal csak a Hivatal által menedzselt vonali kapcsolaton keresztül kommunikálhat (Internet elérés).
b) Az Internetet a belső LAN hálózattal tűzfallal rendelkező router köti össze.
c) Az Internet használata csak a jegyző írásbeli engedélyével (2. számú Melléklet) lehetséges.
d) A Hivatal minden számítógépen folyamatosan bekapcsolt állapotú tűzfalnak kell lennie.

5.3.3 Katasztrófa-helyzetek elhárítása, az üzemfolytonosság biztosítása

5.3.3.1 A Hivatal Katasztrófa esetére az adatmentés kapcsán az alábbiak szerint rendelkezik:

A Zalacsányi Közös Önkormányzati Hivatal

- székhely településén havi rendszerességgel mentett adatokat a Felsőpáhoki Kirendeltség riasztóval védett helyiségben páncélszekrényben,
- míg a Felsőpáhoki Kirendeltségen havi rendszerességgel mentett adatokat a Zalacsányi Kirendeltség riasztóval védett helyiségben páncélszekrényben,
- míg a Nemesbüki Kirendeltségen havi rendszerességgel mentett adatokat a Zalacsányi Kirendeltség szám alatti riasztóval védett helyiségben páncélszekrényben

őrzik, ahol az adatvédelem megoldott; és így az üzemfolytonosság biztosítottá válik.

5.3.4 Az informatikai rendszer külső támogatását biztosító cégek

A Hivatal informatikai rendszerének üzemeltetését támogató mindenkori cégre, valamint más, eseti tevékenységgel megbízott informatikai cégek csak és kizárólag a hardver eszközökkel, az operációs rendszerekkel, az adatbázismotorokkal, valamint a hálózati kommunikáció lehetőségének biztosításával kapcsolatosan felmerülő kérdésekben jogosult probléma megismerésére és megoldási javaslat benyújtására. Hatásköre nem terjedhet ki a kezelt adatbázisokba történő bármilyen betekintésre.

5.3.5 Karbantartás

A megbízható működés fenntartása érdekében az informatikai eszközöket rendszeres tervezett karbantartásnak kell alávetni. A karbantartás során érvényesíteni kell a biztonsági követelményeket, csak előre megtervezett karbantartási folyamat hajtható végre a Hivatal rendszerein, csak az arra jogosult karbantartók végezhetnek karbantartási munkákat.

5.3.6 Oktatás, tájékoztatás

Az informatikai biztonsággal kapcsolatos kockázatok jelentős mértékben csökkenthetők, ha a Hivatal munkavállalói megfelelően ismerik a munkafolyamatokat támogató informatikai rendszereket. A Hivatal minden munkavállalója köteles a hatályos IBSZ-t megismerni, az abban foglaltakat betartani és betartatni.

5.3.7 Ellenőrzések

Az IBSZ-ben foglaltakkal kapcsolatos tevékenységek ellenőrzését a Jegyző látja el. A Jegyző soron kívüli ellenőrzést tarthat, rendelhet el és a rendkívüli események ellenőrzését végezheti. Az informatikai biztonsággal kapcsolatos ellenőrzési feladatok:

a) Vírusellenőrzés. Vírus fertőzés esetén a vírusirtás elvégzése, a fertőzés módjának és eredetének felderítése, valamint a továbbfertőzés megakadályozása.
b) Javító programcsomagok ellenőrzése. A számítógépek operációs rendszereihez tartozó javító programcsomagok telepítése és használatának ellenőrzése.
c) Hálózati megosztások ellenőrzése. A számítógépes hálózatban észlelt, nem engedélyezett hálózati megosztások felderítése és megszüntetése.
d) Számítógépek vizsgálata. A hálózatban üzemelő számítógéppark rendszeres ellenőrzése. Az illegális – nem a Jegyző utasítása alapján telepített és felügyelt – hardver és szoftverek eltávolítása.
e) Mentések vizsgálata. A mentések sikerességének és visszaállíthatóságának ellenőrzése.
f) Hálózati hibakeresés. A rendelkezésre álló eszközök segítségével a Hivatal informatikai hálózatának, hálózati forgalmának figyelése és a műszaki/beállítási hibák vagy illegális tevékenységre utaló jelek felderítése, megszüntetése és a további lehetőségek kizárása.
g) Nyitott portok szűrése. A Hivatal számítógépein található nyitott portok ellenőrzése és a felesleges, nem használt vagy informatikai- és adatbiztonsági veszélyeket jelentő nyitott portok felderítése, és megszüntetése.

Az ellenőrzések lefolytatása a Jegyző utasítása alapján történik. Az ellenőrzés lehet rendszeres vagy eseti ellenőrzés. A vizsgálatok eredményét a jegyző utasításának megfelelően ki kell értékelni, a megállapításokról és a javaslatokról összefoglaló jelentést kell készíteni.

5.3.8 Jelentési és egyéb kötelezettségek

A Hivatal valamennyi munkavállalója köteles minden olyan tudomására jutott eseményt vagy körülményt, amely az informatikai működést veszélyeztetheti, a jegyzőnek azonnal jelezni.

6 Információbiztonsági incidensek kezelése

A Hivatal gondoskodik arról, hogy a biztonsági események és zavarok okozta kár minimális legyen, ennek érdekében az alábbi folyamatokat lépteti életbe az információbiztonsági incidensek kezelésére:

1. Biztonsági események jelentése: ha a Hivatal elektronikus információ-rendszerének bármely komponense vonatkozásában biztonsági esemény

következik be (sérül a bizalmasság, indokolatlan adatmódosítás látható), haladéktalanul tájékoztatni kell a jegyzőt és az informatikai rendszer üzemeltetőt egyaránt, akik döntenek az incidens kezelési módjáról.

2. Szoftverzavarok jelentése: a Hivatal informatikai rendszerének szoftverkomponenseinek feltételezett zavarairól vagy hibajelzéseiről tájékoztatni kell az informatikai rendszer üzemeltetőt, aki biztonsági incidens gyanújának felmerülésekor köteles tájékoztatni a jegyzőt is.
3. Tanulás a biztonsági eseményekből: a biztonsági esemény lezárását követően biztosítani kell, hogy az incidens a jövőben ne fordulhasson ugyanúgy elő, ami a biztonsági intézkedések átalakítását és oktatási feladatokat is maga után vonhat. A követő tevékenységek meghatározása az információbiztonsági felelős feladata.

6.1 Fegyelmi intézkedések

A biztonsági szabályok szándékos megsértőivel szemben a Hivatal belső fegyelmi eljárást indít

Ha bebizonyosodik a számítógépes bűncselekmény tényálladéka, a Hivatalnak meg kell tennie a büntetőjogi feljelentést is (amit csak a Hivatal jogi képviseletét ellátó felelős jogosult megtenni). A fegyelmi eljárásban és a büntetőeljárásban felhasználni kívánt evidenciák megőrzéséről az információbiztonsági felelős köteles gondoskodni.

7 Az IBSZ karbantartása és aktualizálása

Az IBSZ betarthatóságát és aktualitását minden évben felül kell vizsgálni.

Az IBSZ-t módosítani kell, ha

a) felülvizsgálat eredménye, annak betarthatatlanságát állapította meg, vagy olyan külső, illetve belső környezeti változás történt, amely indokolttá teszi azt.

A felülvizsgálatért, a szükséges módosítások átvezetéséért és a hatályba léptetésért a jegyző a felelős.

Zalacsány, 2015. április 30.

Dr. Prótár Henrietta
jegyző

ZALACSÁNYI KÖZÖS ÖNKORMÁNYZATI HIVATAL * Zalacsány *