INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Ásotthalom Nagyközségi Önkormányzat
6783 Ásotthalom
Szent István tér 1.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2017. december 1. napjától

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az Ásotthalom Nagyközségi Önkormányzat és az Ásotthalmi Polgármesteri Hivatal

Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatikai Biztonsági Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az államháztartás szervezetének az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat célja továbbá:

- a titok-, a munka-, a vagyon- és a tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

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

A jelen Informatikai Biztonsági Szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya az államháztartás szervezete valamennyi fő- és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az államháztartás szervezete tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,
- kiterjed az adathordozók tárolására, felhasználására.

3. Fogalmi meghatározások

3.1. Az adatkezelés során használt fontosabb fogalmak

érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést

szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik;

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

3.2. Üzemeltetési fogalmak meghatározása

Hozzáférés (account): a felhasználó azonosítója adott rendszerben. Az account-ot meghatározza: felhasználónév és a jelszó.

Felhasználó (user): az a személy, aki az adott rendszer használatára jogosított account-ot kapott

Bejelentkezés (login): az a folyamat, melyben a felhasználó account adatait egy rendszer számára érvényesítés céljából megadja

Tartomány (domain vagy körzet): rendszeradminisztrációs egység, ahol az account definiálva van

Felhasználói név (user name): az account része, mely a felhasználót az adott rendszerben egyedileg azonosítja

Jelszó (password): a felhasználó által választott betű és/vagy számkombináció, mely a felhasználót igazolja. A házirendben meghatározott szabályoknak eleget kell tegyen

Erőforrás (resource): egy informatikai eszköz szolgáltatása, melyet feladatok elvégzésére fel lehet használni (pl. lemez terület kiszolgálón, hálózati nyomtató, munkaállomás processzorideje stb.)

Rendszergazda: Az a személy, aki adott alkalmazás fölött az összes hozzáférési jogot gyakorolja

Tenant adminisztrátor: Az a személy aki az ASP Keretrendszerben az ASP felhasználókat felvesz és szerepkörök kiosztására van felhatalmazva.

Feladatai:

- új felhasználók (userek) rögzítése,
- meglévő felhasználók adatainak módosítása,
- felhasználók zárolása (szükség szerint),
- felhasználói jogosultságok (szerepkörök) kiosztása,
- felhasználói jogosultságok módosítása, megvonása,
- helyettesítések beállítása, eltávolítása,
- felhasználói csoportok létrehozása, módosítása, törlése (ugyanazon szerepkörök kiosztása több felhasználónak),
- üzleti napló megtekintése (a rendszerben történő változásokat lehet lekérdezni, követni).

4. Az IBSZ biztonsági fokozata

Az államháztartás szervezete adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

Az államháztartás szervezete biztonsági szintje a 3. Az államháztartás szervezete általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési kézikönyv,
- Belső kontroll rendszer.

6. Védelmet igénylő, az informatikai rendszerre ható elemek

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

Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

6.2. 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.

7. A védelem felelőse

A védelem felelőse a Maxentrop Kft.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az államháztartás szervezete adatvédelmi felelősének kell gondoskodnia.

7.1. Adatvédelmi felelős feladatai

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése,
- az adatvédelmi feladatok ismertetése, oktatása,
- a védelmi rendszer érvényesülésének ellenőrzése,
- felelős az államháztartás szervezete informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer önadminisztrációját,

- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- tevékenységéről rendszeresen beszámol az államháztartás szervezete vezetőjének.

7.2. Az adatvédelmi felelős ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

7.3. Az adatvédelmi felelős jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az államháztartás szervezete vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

7.4. Adatvédelmi felelős kiválasztása

Az alábbi követelményeknek kell megfelelnie:

- erkölcsi feddhetetlenség,
- összeférhetetlenség - az adatvédelmi felelős funkció összeférhetetlen minden olyan vezetői munkakörrel, amelyben adatvédelmi kérdésekben a napi munka szintjén dönteni, intézkedni kell.

- az informatika szintjén:
  - = az informatikai hardver eszközök és a védelmi technikai berendezések ismerete,
  - = üzemeltetésben jártasság,
  - = szervezőkészség.
- a szakterületre vonatkozó jogi szabályozás ismerete.

7.5. Az adatvédelmi felelős megbízatása

Az adatvédelmi felelőst a jegyző bízza meg.

Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére az adatvédelmi felelős oktatás formájában biztosítja. Erről nyilvántartást vezet.

Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az államháztartás szervezeténél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.

Az Informatikai Biztonsági Szabályzat folyamatos karbantartása az adatvédelmi felelős feladata.

E tevékenységről, annak konkrét tartalmáról évente egyszer írásbeli beszámolót kell készíteni.

8.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

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

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

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

Ha lehetőség van digitális aláírás használatára, akkor egy digitálisan aláírt példány is elég.

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

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

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

A naplófájlokat havonta át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az államháztartás szervezete vezetőjének azonnal jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a rendszergazda felelős.

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut adatkezelési nyilatkozatot kell aláíratni. (1. sz. melléklet)

Az adatkezelési nyilatkozat naprakészen tartásáért az adatvédelmi felelős *a* felelős.

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).

8.3. Megosztási mappákhoz való hozzáférés

Felhasználói azonosítás az a folyamat, amikor a rendszer a felhasználó által megadott account információ alapján eldönti, hogy az helyes-e, az azonosítást kérő személy rendelkezik-e érvényes account-tal.

Azonosítás két szinten történhet.

– Hálózati szinten
  A felhasználó egy hálózati rendszerbe vagy egy kiszolgálóra jelentkezik be

– Alkalmazás szintjén
  Ha a felhasználó által használni kívánt alkalmazás (program) saját hitelesítési rendszerrel rendelkezik, akkor az ott érvényes felhasználói paraméterekkel jelentkezik be.

8.3.1. Windows hálózati bejelentkezés

Az Ásotthalmi Polgármesteri Hivatal által használt hálózati rendszerben az azonosítás olyan account információ felhasználásával történik, melynek részei

- a felhasználói név
- jelszó

melyek együttesen érvényesek. A felhasználói neveket meghatározott szabály szerint, a rendszergazda hozza létre a jegyző utasítására.

8.3.2. Alkalmazás szintű bejelentkezés

Az ASP alkalmazás futtatásához vagy annak adatainak eléréséhez felhasználói azonosításra van szükség, mivel az alkalmazás önálló felhasználó-kezeléssel rendelkezik, ezért alkalmazás szintű bejelentkezésre van szükség.

Ebben az esetben a program használatához a hálózatitól eltérő account-ot kell beszerezni, amelyet az ASP rendszer generál, miután a Tenant adminisztrátor regisztrálta a felhasználói jogosultságait.

Az ASP elsődleges autentikációs eszköze az eSZIG. A használatához javasolt kártyaolvasók hatóság által bevizsgált és elfogadott eszközök. Az elektronikus személyigazolvánnyal történő authentikáció során a következő szabályzókra kell megkülönböztetett módon figyelni:

- Minden ASP rendszert használó munkatársnak rendelkeznie kell eSZIG-el.
- Az eSZIG használatához szükséges a kártyaolvasó számítógépre történő telepítése.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rögzített felhasználói fiók és az eSZIG összerendelése szükséges.
- A személyi igazolvány kártyát csak a tulajdonosa használhatja, azt ASP rendszer authentikációs folyamat céljából másnak átadni tilos.

- Az hivatal vezetőjének a Jegyzőnek gondoskodnia kell arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen.
-

8.4. Hozzáférés igénylése

A hozzáférést minden esetben igénylőlap (adatlap) benyújtásával kell megkérni.

Az igénynek tartalmaznia kell:

- a felhasználó pontos adatait
- a szükséges szolgáltatásokat és jogosítások szintjét

Az igénylőlapot a költségvetési szerv vezetőjének kell címezni jóváhagyásra. Jóváhagyás nélküli igényeket a rendszergazda nem teljesíti.

8.5. Account átvétele

- az elkészült account kézbesítéséről az rendszergazda gondoskodik
- az account átadása kizárólag annak tulajdonosának történhet

8.6. Az account kézbesítésének módjai:

A felhasználó érdekeinek védelmében az account átvételekor egy jelszó kerül átadásra, mely nem megváltoztatandó. Alkalmazások felhasználói számára a jelszócsere ajánlott *(amennyiben lehetséges).*

8.7. Az account felhasználási feltételei

A személyre szólóan kiadott jelszót a felhasználó köteles titokban tartani. Másnak átadni, leírni, vagy egyéb formában rögzíteni tilos!

Az államháztartás szervezetének vezetője beosztottját jelszavának átadására nem utasíthatja.

A szervezet hálózatában, alkalmazásaiban, rendszereiben használt jelszavak nyilvános hálózatban való (Internet) használata nem javasolt.

A felhasználó nem hagyhatja felügyelet nélkül azt a munkaállomást/alkalmazást, melyre bejelentkezett.

Ha munkaállomástól/alkalmazástól eltávozik, köteles azt a munkaállomás zárolásával (Lock Workstation) védeni.

Hosszabb időtartamra való távozás esetén (pl. munkanap/műszak vége) az alkalmazásból és a munkaállomásról is ki kell jelentkezni, a munkaállomást ki kell kapcsolni, kivétel, ha a rendszergazda másképpen nem rendelkezik.

8.8. Hozzáférés korlátozása (account zárolása)

A biztonsági előírások és a költségvetési szerv érdekei megkövetelik, hogy visszaélések és azok gyanúja esetén a felhasználó rendszerhez/hálózathoz/alkalmazáshoz való hozzáférése korlátozva legyen.
Korlátozások életbe léphetnek automatikusan, vagy a rendszergazda kezdeményezésére a költségvetési szerv vezetőjének jóváhagyásával.

8.9. Manuális korlátozások

- account jogosulatlan használatakor
- jogosultságokkal való visszaélés, károkozás esetén
- a munkavégzésre irányuló jogviszony megszűnésekor
- az alkalmazott, egyéb foglalkoztatott felettesének indokolt kérése alapján

9. Az informatikai eszközbázist veszélyeztető helyzetek

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.

9.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
  - földrengés,
  - árvíz,
  - tűz,
  - villámcsapás, stb.
- Környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának felszökése vagy leesése,
  - piszkolódás (pl. por).

- Közüzemi szolgáltatásba bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- illegális másolattal vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Az államháztartás szervezete a munkavégzés során használt számítógépek kiemelt adatait az alapján lehet megállapítani, hogy az egyes gép, mely alkalmazási területen van jelen.

Általánosságban megállapítható, hogy az összes hivatali számítógépen tárolt Microsoft Office dokumentumok, legyen az Word, Excel vagy PowerPoint prezentáció, védett anyagnak minősül.

Amennyiben az említett dokumentumok valamelyike nem elérhető a felhasználó számára, az adatvesztésnek tekinthető.

Védett adatnak minősül továbbá a felhasználói levelezés is, mely nemcsak a fogadott leveleket érinti, hanem a felhasználó által kiküldött leveleket is.

Ezek alapján a következő fájltípusokat tekinthetjük védett adatoknak:
- .doc, .xls, .ppt, .pps
- .pdf
- .eml, .dat, .pst, .ost, .pad

10.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

10.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

10.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

11. Az informatikai eszközök környezete, azok védelme

11.1. A szerverszoba minimális igénye

- a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,
- a lehető legkevesebb nyílászáróval kell rendelkeznie,
- váratlan áramkimaradás esetén a szerver*(eke)*t intelligens UPS –sel kell ellátni (szünetmentes tápegység), mellyel az áramkimaradás folyamatosságát biztosítani lehet.

11.2. A munkaállomásokra vonatkozó előírás

Csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót bezárva kell tartani.

11.3. Egyéb vagyonvédelmi előírások

- a gépterem *(szerverszoba)* külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a szerverszobába való be- és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak a gépteremben,
- a szerverszoba kulcsának felvétele, illetve leadása csak aláírás ellenében történhet,
- munkaidőn túl a szerverszobában csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a szerverszobába történő illetéktelen behatolás tényét az államháztartás szervezte vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

11.4. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (floppy, CD, DVD, pendrive) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
- adathordozót más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.5. Vírus védelem

11.5.1. Vírusfertőzés gyanús helyzetek

Sok jele lehet vírus jelenlétének, azonban ezek nagy része normál tevékenység eredményeként is előállhat. Mivel a vírusok írói általában igyekeznek elkerülni a feltűnő viselkedést, a felhasználó nem feltétlenül találkozik az alább felsorolt – vírusfertőzésre utaló – jelenségekkel:

- A víruskereső program névvel azonosított vírust jelez. A lehető legerősebb vírusjegy.
- Fájl másolása esetén az újonnan keletkezett és az eredeti példány hossza eltérő.

  Nagyon erős vírusjegy.
- Szokatlan és váratlan képernyő tevékenység (szokatlan üzenetek, ablakok megjelenése). Erős vírusjegy.
- Szokatlan számítógép- vagy programviselkedés (pl. programok maguktól elindulnak). Általánosan erős vírusjegy. Ha az operációs rendszer újraindítása után is fennáll, erős vírusjegynek tekinthető.
- A rendszer működése többszöri újraindítás után is egyértelműen lassabb a megszokottnál. Átlagosan erős vírusjegy. Helytelen rendszerkonfiguráció is okozhatja.

11.5.2. Teendők vírusfertőzés esetén

Tájékoztatni kell a vírusvédelemért felelős személyt *rendszergazdát* a fertőzésről vagy annak gyanújáról.

A számítógépet újra kell indítani egy előkészített, vírusmentes, a használt operációs rendszert és a vírusvédelmi program legfrissebb változatát tartalmazó lemezről. Ha ez nem lehetséges, akkor védett módban kell újraindítani a gépet csak a legszükségesebb szolgáltatásokkal (lehetőleg hálózati kapcsolat nélkül).

A vírusvédelmi szoftvert elindítjuk, és megszüntetjük a vírusfertőzést. Ez történhet elsődlegesen a fertőzött állomány javításával (a vírus eltávolítása), ha erre lehetőség van, egyébként a fertőzött állomány törlésével. Ez utóbbi esetben ügyelni kell arra, hogy nem rendszerállományról van-e szó.

A víruskeresést addig kell végezni, amíg el nem éri a rendszerfelelős, hogy a víruskereső program úgy fusson végig az összes állományon, hogy fertőzött állományt már nem talál. Ezek után a rendszer újraindítható a szokott módon.

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.
- 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.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.
- A felhasználók részéről tilos a vírusellenőrző szoftver beállításainak módosítása.

11.6. Tűzvédelem

A gépterem (szerverszoba) illetve kiszolgáló helyiség az alacsony kockázati osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a gépteremre *(informatikai szobára)* vonatkozóan az államháztartás szervezete Tűzvédelmi szabályzata tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a gépterem és az adatállomány-tároló helyiség között.

Az államháztartás szervezete azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A gépteremben csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. leporellót).

A gépteremben dohányozni tilos!

Az n, valamint a munkaállomásoknál ételt, italt fogyasztani tilos!

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

Ezen adatállományok kijelölése az adatvédelmi felelős feladata.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A gépterem (szerverszoba) védelme

Elemi csapás *(vagy más ok)* esetén a gépteremben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

12.2. 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 gyártó előírásait, ajánlatait,
- a tapasztalatokat,
- a hardver tesztek által feltárt hibákat.

Alapgép szétbontását (kivéve a garanciális gépeket) csak a rendszergazda végezheti el. Billentyűzet, monitor, nyomtató cseréjének idejét dokumentálni kell.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítés szoftver védelme. A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.
- hozzáférési lehetőség:
  - = a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
  - = az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.

  A szerver*(ek)* rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontását dokumentálni kell.
- adatrögzítési folyamat bizonylatolása.

  A másodlagos adathordozókat kísérő jeggyel kell ellátni melynek tartalma:
  - témaazonosító, bizonylat neve,
  - rekord (tételszám),
  - rögzítést ill. ellenőrzést végző személyek nevei.
- adatrögzítés folyamatához kapcsolódó dokumentációk:
  - = adatrögzítési utasítások,
  - = ellenőrző rögzítési utasítások,
  - = tesztelő és törlő programok kezelési utasításai,
  - = megőrzési utasítások,
  - = gépkezelési leírások.

12.3.2. Adathordozók védelme

Az államháztartás szervezetében az alábbi adathordozók lehetnek: floppy, CD lemez, DVD lemez, mikrofilm, pendrive, hordozható winchester, notebook, asztali számítógép, szerver, okos telefon, stb.)

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani.

Az informatikai eszközök üzemeltetéséért a *rendszergazda* felelős.

Köteles gondoskodni a feldolgozások igényeinek megfelelő 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.

Az operációs rendszer adta lehetőségek figyelembevételével biztosítani kell a külső és belső címek azonosságát.

A belső címke felépítésével, illetve használatánál figyelembe kell venni a megőrzési időpont ellenőrzésének szükségszerűségét (aktuális ellenőrzés).

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

12.3.3. Adathordozók tárolása

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

Mágneses adathordozót a részlegből ki-, illetve oda bevinni csak a jegyző engedélye alapján lehet.

12.3.4. Az adathordozók nyilvántartása

Az adathordozókról nyilvántartást kell vezetni.

A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.

A nyilvántartás vezetéséért: gazdálkodási ügyintéző pénztáros felelős.

12.3.5. 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 az államháztartás szervezete Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

12.3.6. Az adathordozók karbantartása

Az adathordozókat 1 évenként *(félévenként)* tisztítani kell és ellenőrizni a mágneses adathordozók állapotát, elöregedését.

12.3.7. 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 (deformálódott) mágneslemezt, CD-t, DVD-t, pendrive-t.
- véglegesen elhasználódott anyagot *(pl. leporelló).*

Az alkalmatlan mágneslemezeket, CD-ket, DVD-ket, pendrive-ket fizikai roncsolással használhatatlanná kell tenni.

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

A selejtezésről 3 példányban jegyzőkönyvet kell készíteni, melynek az alábbi adatokat kell tartalmaznia:

- a selejtezendő adathordozók tulajdonosának megnevezését,
- a selejtezés időpontját,
- milyen adathordozók, és azok mely adatai kerülnek selejtezésre,
- a selejtezést végzők aláírását.

A selejtezési jegyzőkönyvek nem selejtezhetőek.

Titkos adatokat tartalmazó adathordozókat selejtezni nem lehet, ezen adatokat tartalmazó adathordozókat a TÜK utasítása szerint kell kezelni.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. *(Az üzemi másolás nem minősül másolásnak.)*

Biztonsági illetve archív adatállomány előállítása másolásnak számít.

12.3.8. Leltározás

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

12.3.9. Mentések, file-ok védelme

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

A mentések folyamata:

- A mentéseket naponta, központi mentő szoftverrel kell végrehajtani.
- A mentésből a rendszerek, a szoftverkörnyezet beállításainak, valamit a tárolt adatoknak teljeskörűen visszaállíthatónak kell lennie a mentés pillanatának állapotára.
- A szerverek esetében az adatokat legalább 2 példányban kell menteni, és egymástól fizikailag elkülönült helyiségben elzárt, a szerverterem tűzterétől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A szerverek mentését legalább *hetente*, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni.
- A szerveren működő WEB oldalak mentése a rendszergazda feladata. A mentést minden módosítás után el kell végezni.
- A mentett adatokhoz csak az arra jogosultak férhetnek hozzá.

Az egyéb mentéseket meghatározott időszakonként el kell végezni.

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

Az online működő szoftverek esetében a mentés a szoftver üzemeltetőjének feladata.

A költségvetési könyvvezetés és a pénzügyi könyvvezetés adatai az ASP rendszer a rendszer működtetőjének feladata.

A levelezések mentését vagy a felhasználó, vagy kérésre a rendszergazda végzi el.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adathordozókról másolatot kell időnként készíteni.

A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

Az üzemeltetésért felelős vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Teendők a következők:

- az üzembiztonság érdekében tartalék operációs rendszerrel kell rendelkezni, amely szükség esetén azonnal betölthető legyen,
- a rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges,
- név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek,
- a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni,

– a változtatásokról nyilvántartást kell vezetni.

12.4.2. Felhasználói programok védelme

12.4.2.1. 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 programját. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

A jelszavaknak az alábbi minimális követelménnyel kell rendelkeznie:

- A hálózati jelszó legalább 8 karakterből álljon, kis és nagybetűk, valamint számok, egyéb írásjelek közül legalább 2 típusút tartalmazzon.
- Az alkalmazáshoz szükséges jelszavaknak legalább 5 karakterből kell állni.
- A jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, vagy könnyen visszafejthető kifejezéssel.
- A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat havonta meg kell változtatniuk.
- Ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.
- A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt 5 jelszóval.
- A jelszót nem szabad több személy között megosztani.
- A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.
- A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.
- A jelszavakat, valamint a munkaállomások BIOS jelszavát lezárt, aláírt és lepecsételt borítékban páncélszekrényben *(lemezszekrényben)* kell tárolni, lehetőleg a vezető irodájában.

Gondoskodni kell arról, hogy a tárolt programok, file-ok 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 program azonosítója,
- a program készítőjének neve,
- a feldolgozási rendszer megnevezése.

A program dokumentáció a rendszerdokumentációnak része.

12.4.2.2. Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni,
- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében az államháztartás szervezete az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

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

12.4.2.3. Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni a programkönyvtárba elhelyezett programokról.

12.5. Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezettségű dokumentálásnak.

A dokumentációról nyilvántartást kell vezetni, s ennek az alábbiakat kell tartalmaznia:

- rendszer megnevezése,
- dokumentáció típusa,
- a rendszer adatvédelmi minősítése,
- a kidolgozók névsora,
- példányszám és tárolás helye,
- az átadás ideje,
- módosítások megnevezése és ideje.

13. A központi számítógép*(ek)* és a hálózat munkaállomásainak működésbiztonsága

13.1. Központi gép (Server)

Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A központi gép háttértárairól hetente egy teljes, a többi napon különbségi biztonsági mentést kell készíteni. A mentéseket heti egy alkalommal külső adattároló egységre kell másolni. Az így keletkezett heti mentéseket 5 évig meg kell őrizni.

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.

13.2. Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet.

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 előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

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

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

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 munkaállomások nincsenek jól védhető helyen, ezért védelmükről szoftver úton gondoskodni kell.
- Ha a felhasználó napközben magára hagyja a gépet, zárolást, vagy jelszavas képernyővédőt kell alkalmaznia.
- Ha a felhasználó munkaviszonya megszűnik, akkor felhasználói azonosítóját meg kell szüntetni.

14. Internet hozzáféréssel kapcsolatos intézkedések

Az internet eléréseket biztosító számítógépekre a helyi hálózatra nem kapcsolódó munkaállomásokra vonatkozó szabályok érvényesek.

Az internetes gépen minden esetben működtetni kell a vírusvédelmet.

A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.

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

A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztését a jegyző szabályozza.

15. Az elektronikus levelezés szabályai

Minden alkalmazottnak szükséges internetes postafiókot igényelni, és ezt kizárólag hivatali célokra engedélyezett használni, amely: felhasználó.név@asotthalom.hu formátumú.

Az államháztartás szervezete nem monitorozza a hálózatából küldött, illetve ide érkező levelek tartalmát.

Az államháztartás szervezte hálózatán átmenő leveleken központilag vírusellenőrzés történik, ami különböző védelmi és szűrési funkciókkal egészül ki.

Az elektronikus levelezés alapelvei:

- A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartásformát.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelek tartalma nem sérthet meg szerzői és szomszédos jogokat.
- A levelek nem ronthatják az államháztartás szervezete hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.
- Tilos kéretlen leveleket, hirdetéseket küldeni.
- Tilos a levélbombák, levelezési láncok küldése, illetve továbbküldése.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
- Tilos a levelezési címet olyan kereskedelmi listára feltenni, amelyről az államháztartás szervezete levelező rendszerét e-mail szeméttel (spam) terhelhetik meg.

A hálózaton történő (titkosítás nélküli) levelezés nem biztonságos, könnyen megfigyelhető (akárcsak egy levelezőlap tartalma), ezért érzékeny információkat titkosítás nélkül soha ne küldjünk e-mailben.

Ismeretlen feladótól érkezet, különös témájú, csatolt fájlt tartalmazó levelekkel legyünk nagyon óvatosak, a jelek vírusfertőzésre utalhatnak, töröljük a levelet.

15. Ellenőrzés

Az államháztartás szervezete éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.

A folyamatba épített előzetes, utólagos és vezetői ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

ASP-vel kapcsolatos audit tevékenység csak a Hatóság írásbeli engedélyével végezhető el. Erről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.

ASP rendszeren külsős Fél, szervezet nem végezhet sérülékenységi vizsgálatot a Hatóság írásbeli engedélye nélkül. Ezen vizsgálati tényről az önkormányzat tájékoztatást ad a Magyar Államkincstár részére.

16. Záró rendelkezések

Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat, melyet 2017. év december 31.napjáig kell elvégezni.

A szabályzatot jogszabályi vagy szervezeti változás esetén 90 napon belül módosítani kell.

A munkaköri leírások elkészítésért, aktualizálásáért a jegyző felelős.

Az Informatikai Biztonsági Szabályzat

2017. év. december hó 1.–napjával lép hatályba.

Ezzel egyidejűleg a ..... -én hatályba lépett IBSZ hatályát veszti.

Ásotthalom, 2017. november 30.

Toroczkai László
Polgármester

Ásotthalom Nagyközségi Önkormányzat Csongrád megye

Dr. Hajnal Péter
Jegyző

1. sz. melléklet

ADATKEZELÉSI NYILATKOZAT

Alulírott ..... (név)

..... (lakcím) nyilatkozom, hogy a feladatellátás során tudomásomra jutott információkat megőrzöm, azt illetéktelen személyek részére nem adom át.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáférésére kísérletet sem teszek.

Dátum: 201... .....

.....
aláírás

2. sz. melléklet

GÉPTERMI REND

1. A gépteremben (szerverszobában) és az adatrögzítő helyiségében az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:

   - az államháztartás szervezete vezetője
   - szervezők, programozók, műszaki szakemberek.

   Más személyek benntartózkodását csak az államháztartás szervezete vezetője engedélyezheti.

2. Üzemeltetés alatt az ajtókat állandóan becsukva, üzemidőn kívül pedig zárva kell tartani és a kulcsokat le kell adni.

   A gépterem kulcsát csak a jegyző által összeállított külön listán szereplő személyek kaphatják meg.

   Munkaidőn kívül idegen személy csak az államháztartás szervezete vezetőjének (távollétében helyettesének) engedélyével tartózkodhat a gépteremben.

   A gépterem és az adatrögzítő helyiség áramtalanításáért a műszakban kijelölt gépkezelő a felelős.

3. A gépteremben az esztétikus, higiénikus, folyamatos munkavégzés feltételeit meg kell őrizni. A géptermi rend megtartásáért ....., a biztonságos műszaki üzemeltetésért ..... a felelős.

4. A gépterembe ételt, italt bevinni és ott elfogyasztani TILOS !

5. SZIGORÚAN TILOS a gépteremben égő cigarettával belépni, illetve ott dohányozni!

6. A gépterem takarítását csak az arra előzőleg kioktatott személyek végezhetik.

7. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak ..... végezheti. Ez alól csak a szervizek szakemberei kivételek.

8. Az informatikai eszközöket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.

9. A gépteremben elhelyezett adathordozókhoz ..... *(gépkezelőkön)* kívül, illetve azok engedélye vagy jelenléte nélkül senki nem nyúlhat.

10. Mágneslemezeket, CD és DVD lemezeket, pendrive-ket, leporellókat csak a gépkezelő engedélyével lehet kihozni, illetve bevinni a gépterembe.

11. Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet!

12. A gépteremben elhelyezett jelzőberendezések *(klíma, tűz- és betörésjelző)* műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak, és bármilyen rendellenességet észlelnek azonnal jelenteni kell a működésükért felelős megbízottaknak.

13. A gépteremben egyszerre legalább egy, a gépek kezeléséhez értő személynek kell tartózkodnia. Üzemben lévő géptermet felügyelet nélkül hagyni nem szabad!

14. A javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

A fenti rendelkezések megsértése esetén fegyelmi felelősségre vonás kezdeményezhető.

Megismerési nyilatkozat

A *Az* Ásotthalom Nagyközségi Önkormányzat, és intézménye:

- Ásotthalmi Polgármesteri Hivatal

az informatikai biztonsági szabályzatában foglaltakat megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartatni.

Név	Feladat, hatáskör	Dátum	Aláírás
LAKATOS-PAPP ANNA IBOLYA	gazd. ü.i.	2017. 11. 30.	L-Papp Anna
GAJDÁCS EDIT	gazd. ü.i.	2017. 11. 30	Gajdács Edit
SZÍRINGERNÉ GORA KATALIN	gazd. ü.i.	2017. 11. 30.	Szíringerné Gora Katalin
PIPICZNÉ WOLFORD ERIKA	gazd. ü.i.	2017. 11. 30.	Pipiczné Wolford Erika
KÓSZONÉ KÓSZÓ ARANKA	adóü.i. ü.i.	2017. 11. 30.	Kószoné Kószó Aranka
PÉTEK NÓRA	szoc. és [illegible] ü.i.	2017. 11. 30.	[illegible]
FARKASNÉ KIRI KLÁRA	személyzeti ü.i.	2017. 11. 30	[illegible]
Pipicz Anita	gazd. ü.v.	2017. 12. 11.	[illegible]
FÖDI JÓZSEFNÉ	hat., települési ü.i.	2017. 11. 30.	Födi Józsefné
MITRÓKNÉ KRISZTIN ERIKA	ált. ig. ü.i.	2017. 11. 30.	[illegible]
DOBOSNÉ KISMÁRTON TÜNDE	adóü.i. ü.i.	2018. 03. 01.	Dobosné Kismárton Tünde