IBSZ

ERDŐKERTESI PMH

AZ ERDŐKERTESI POLGÁRMESTERI HIVATAL
INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

I.
AZ ERDŐKERTESI POLGÁRMESTERI HIVATAL INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Az Erdőkertesi Polgármesteri Hivatalnak Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) az informatikai rendszerrel kapcsolatos adatvédelem és adatbiztonság megteremtése érdekében - információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI. 22.) KSH rendelkezésben foglaltak figyelembe vételével - az alábbi intézkedést adom ki:

1. Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és 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 üzembe helyezésen keresztül az üzemeltetésig.
A jelen IBSZ 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 kiterjed az adott hivatalra.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed a hivatal tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- 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. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

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

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:

- Leltározási és értékelési szabályzattal,
- Számviteli politikával

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:

- 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,

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 mindenkori informatikai vezető és rendszergazda/ák.
A jelen szabályzatban foglaltak szakszerű végrehajtásáról a hivatal vezetőinek kell gondoskodnia.

7.1. Adatvédelmi felelősök feladatai

a) Informatikai vezető feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,

- ellenőri tevékenységét adminisztrálja.
- ellenőrzi a szoftverek használatának jogszerűségét

b) Rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok
- készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a hivatal informatikai rendszer hardver eszközeinek karbantartásáért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját,

7.2. Az informatikai vezető 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 informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a hivatal 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,
- az informatikai beruházásokat véleményezi.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
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 a hivatalnál - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az informatikai vezető feladata.

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.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi 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.
Az információhoz való hozzáférést lehetőség szerint 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 rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a hivatal vezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.

Az 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).

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,
- 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

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 környezetének védelme

11.1. Vagyonvédelmi előírások

- a gépterem helyiségét biztonsági zárral kell felszerelni,
- a gépterembe való be- és kilépés rendjét szabályozni kell,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét a hivatal vezetőjének
- azonnal jelenteni kell,
- az informatikai eszközöket csak a hivatal arra felhatalmazott alkalmazottai használhatják,
- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

11.2. 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 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 másnak átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.3. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
A hivatal szerverszobájába legalább 1 db tűzoltó készüléket kell elhelyezni, itt elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.
A nagy fontosságú, pl. törzsadat-állományokat két példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A számítógépek és szerverek védelme

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

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- 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 üzemeltetést, karbantartást és szervizelést az informatikusok végzik.
- A munkák szervezésénél figyelembe kell venni:
- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.
- Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.
-

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 adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek
- rendelkeznek ellenőrző funkciókkal és biztosítják 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 személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető kezeli.
  Az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

12.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

12.3.3. Adathordozók tárolása

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

12.3.4. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylatőrzési kötelezettségnek megfelelően kell kialakítani

12.3.5. Selejtezés, sokszorosítás, másolás

A selejtezést a hivatal selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

12.3.6. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

12.3.7. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

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

12.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.
Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősnek naprakész nyilvántartást kell vezetni
A számvitelről szóló többször módosított 2000. évi C. törvény értelmében az adott 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 vezetők a felelősek.

13. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

13.1. Központi gépek

Szünetmentes áramforrást szükséges használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.
Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.
A vásárolt szoftverekről biztonsági másolatot kell készíteni.

13.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A hivatal 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 csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

14. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

15. Záró rendelkezések

Erdőkertes Polgármesteri Hivatal jegyzője jelen szabályzatot adja ki. Jelen szabályzat az Erdőkertesi Polgármesteri Hivatal Ügyrendjének mellékletét képezi.
Az Informatikai Biztonsági Szabályzat 2013. október 1-én lép hatályba.
Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat**.**

Erdőkertes, 2013. szeptember 30.

Vargáné Rajna Ágnes
címzetes főjegyző

II.

Felhasználói biztonsági szabályzat

Az Erdőkertesi Polgármesteri Hivatal (továbbiakban hivatal) a munkavégzéshez megfelelő számítástechnikai hátteret biztosít, a biztosított eszközöket azonban kizárólag munkavégzés céljára lehet használni.
A biztosított eszközök a hivatal tulajdonát képezik.

Eszközökkel kapcsolatos szabályok

- Amennyiben a felhasználó bármilyen biztonsági problémát vagy hibát észlel azonnal köteles értesíteni a rendszergazdákat.
- Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.
- Tilos az eszközök közelében enni, inni, dohányozni.

Jelszókezeléssel kapcsolatos szabályok

- A felhasználó háromhavonta köteles jelszavait lecserélni.
- A jelszó minimum nyolc karakter hosszú, (kicsi és nagy) betűket és számokat is kell tartalmaznia.
- A jelszó nem írható le semmilyen jól látható, vagy könnyen hozzáférhető helyre.
- Tilos a névre szóló jelszó kiadása más felhasználók számára.

Szoftverekkel kapcsolatos szabályok

- A hivatal kizárólag jogtiszta szoftverekkel dolgozik.
- A jogtisztaság biztosítása a hivatal vezetőinek felelőssége, ezért tilos a hivatal informatikai munkatársain kívül bármely más felhasználónak bármilyen terjesztési engedéllyel (freeware, shareware, stb.) rendelkező szoftvert, a cég tulajdonát képező számítógépre feltelepíteni. A szoftverek törlését is csak hivatal informatikus munkatársai végezhetik el. Ez alól kivételt képeznek a víruskeresők, melyek fertőzés esetén jogosultak a számítógépről fájlokat törölni.

Adatvédelmi szabályok

- A felhasználók számára tilos bármilyen adathordozóra adatokat lementeniük a számítógépükről vagy a szerverekről. Külső adathordozót (Pen drive, CD/DVD stb.), csak a hivatal informatikus munkatársai csatlakoztathatnak a számítástechnikai eszközökhöz.
- A munkahely elhagyása esetén a számítógépet zárolni kell a "Windows" + "L" billentyűk egyidejű lenyomásával, illetve olyan képernyővédőt kell beállítani, melyek jelszóval engedik csak a gép feloldását.
- A személyes, munkához közvetlenül nem kapcsolódó állományok tárolása mind a munkaállomásokon, mind a szervereken nem engedélyezett.

- A számítógépen tilos mappa megosztást definiálni, működtetni. Kivétel ez alól a minden számítógépen létrehozott osztott mappa. Használatuk kizárólag arra az esetre vonatkozik, amikor a számítástechnikai eszközök között adatállomány-mozgatás történik. Ezen mappákban tilos állományokat tárolni!

Internethasználattal kapcsolatos szabályok

- Tilos a munkahelyen minden valós idejű kommunikációs program használata. Idetartozik az MSN, ICQ, IRC, és egyéb hasonló üzenetküldő használata. Tilos továbbá web-felületen keresztül elérhető valós idejű üzenetküldő úgynevezett "chat" program használata. Indokolt esetben az informatika osztály jogosult központilag tiltani ezen alkalmazásokhoz szükséges feltételeket.
- Tilos a munkahelyi Internet kapcsolaton keresztül minden olyan program és egyéb fájlletöltése, ami nem a munkavégzéshez szükséges.
- Tilos minden Internetes "online" sugárzott műsor (ide tartoznak a rádió, televízió műsorok) hallgatása, megtekintése az Internet sávszélesség indokolatlan csökkentése miatt. Az informatikai rendszer vezetői, a rendszergazda jogosult az Internet kapcsolat sávszélességének és forgalmának ellenőrzésére, korlátozására, amennyiben azt valamilyen konkrét észrevétel indokolja, hogy az Internet kapcsolat optimális kihasználtságát, vagy a munkát hátráltatja.
- Mindenféle fájlmegosztó alkalmazás használata a hivatal számítástechnikai eszközein tiltott.

Vírusvédelmi szabályok

- A számítógépen vírusellenőrző program fut, mely a gép működése közben automatikusan figyeli a rendszert. A vírusellenőrző programot leállítani és annak működésébe beavatkozni szigorúan tilos.

- Minden fájlművelet előtt ez a program ellenőrzi a megnyitott fájlokat. Bármilyen, adatbiztonságot veszélyeztető esemény figyelmeztetése jelenik meg a felhasználó monitorán, azonnal értesítenie kell a rendszergazdát, hogy a megfelelő lépésekkel megakadályozhassa a kártékony programok további fertőzéseit. Ugyanerről az eseményről a vírusirtó program

- elektronikus üzenetet küld rendszergazdák számára.

- Vírustalálat esetében a munkát azonnali hatállyal fel kell függeszteni, a számítógépet az adathálózatról le kell választani és megkezdeni az okok feltárását és a helyreállítást.

1.sz.melléklet

Felhasználói nyilatkozat

Számítástechnikai Felhasználói Biztonsági Szabályzatot elolvastam, tudomásul vettem és elfogadom.

Munkáltató megnevezése: ***Erdőkertesi Polgármesteri Hivatal***

Név (nagybetűvel):……..

Munkakör:…….

Dátum: 2013. ……..

Aláírás:

…….

A Felhasználói nyilatkozat átvettem:

Név (nagybetűvel):……..
személyügyi felelős

Munkáltató megnevezése: ***Erdőkertesi Polgármesteri Hivatal***

Dátum: 2013. ……..

Aláírás:

2. sz. melléklet

ADATKEZELÉSI NYILATKOZAT

Erdőkertesi Polgármesteri Hivatal

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.

Kelt: Erdőkertes, 2013. ……..

……
aláírás

Jogszabályok és szakirodalmi áttekintés

Vonatkozó hazai jogszabályok

1968 évi I. törvény - A szabálysértésekrôl.
1978. évi IV. törvény - A Büntető Törvénykönyvrôl.
1987. évi XI. törvény - A jogalkotásról.
1990. évi X. törvény - A különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról.
1991. évi LXIX. törvény - A pénzintézetekről és a pénzintézeti tevékenységről.
1992. évi LXIII. törvény - A személyes adatok védelméről, a közérdekű adatok nyilvánosságáról.
1992. évi LXVI. törvény - A polgárok személyes adatainak nyilvántartásáról.
1987. évi 5. törvényerejű rendelet - Az állam és szolgálati titok védelméről.
17/1987. (VI. 9.) MT rendelet - Az 1987. évi 5. törvényerejű rendelet végrehajtásáról.
26/1990. (II.14.) MT rendelet - A nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról.
61/1990. (X.1.) Korm. rendelet - Az egyes nemzetközileg ellenőrzött termékek és technológiák forgalmának engedélyezéséről.
1026/1992. (V.12.) Kormányhatározat - A közigazgatás korszerűsítési programjáról.
1039/1993. (V.21.) Kormányhatározat - A központi államigazgatási szervek informatikai fejlesztéseinek koordinálásáról.

Tájékoztató jogszabályok

Az Osztrák Szövetségi Köztársaság Adatvédelmi Törvénye (Bundesgesetzblatt Nr. 565/1978. és Nr. 370/1986.)
Törvény az adatvédelem és az adatfeldolgozás fejlesztésérôl - NSZK (Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990. BGBI. I. 2954.)
Külföldi hírszerzôi tevékenység megfigyeléséről szóló törvény - USA (Foreign Intelligence Surveillance Act of 1978. 1978 U.S.C. 1901)
A telefonszámlákhoz, a telefonhasználatot regisztráló nyilvántartásokhoz való kémelhárítási célú hozzáférésrôl (Counterintelligence access to telephone tools and transaction records (USA) Section 2709 of title 18, United States Code)
Hírközlési törvény - USA (Communications Act 47 U.S.C. 605)
A számítástechnikai eljárás védelméről szóló törvény - USA (Computer Security Act 52 U.S.C. 1321)

Szabványok, ajánlások

UK. GOSIP 3.0 Part IV. Data Interchange
Electronic Data Interchange (EDI) Standards, DATAPRO Managing Data Networks 8430 (August 1991)
CCITT Recommendation X.400, DATAPRO Managing Data Networks 8426 (Februáry 1991)
EPHOS 7.0 (X.400 és FTAM leírásai)

"Information Technology Security Evaluation Criteria (ITSEC)" Version 1.2, May 1991, EC DG XIII.
"Information Technology Security Evaluation Manual (ITSEM)" draft version 0.2, April 1992, EC DG XIII.
"Trusted Computer Systems Evaluation Criteria (TCSEC) US Department of Defense, 1983
"Information Security INFOSEC'92 Security Investigations" 1992, EC DG XIII.
"Information processing systems. Open Systems Interconnections. Basic Reference Model. General requirements" - ISO 7498: 1984.
"Information processing systems. Open Systems Interconnections. Basic Reference Model. - Part 2: Security Architecture" - ISO 7498-2: 1989 (E)
ISO 9070: 1991. Information Technology - SGML support facilities - Registration procedures for public text owner identifiers
FIPS PUB 161, Electronic Data Interchange (March 1991)
CCITT Recommendation X.400 - 1984, Message Handling Systems: System Model - Service Elements, and related documents in this series.
CCITT Recommendation X.400 - 1988, Message Handling, System, and Service Overview, and related documents in this series.
CCITT Recommendation X.435 - 1991, Message Handling Systems: EDI Messaging System.
CCITT Recommendation X.800 - 1991, Security architecture for OSI for CCITT applications.
X12.22 Data Segment Directory
X12.3 Data Element Dictionary
X12.42 Cryptographic Service Message
X12.5 Interchange Control Structure
X12.56 Interconnect Mailbag Control Structures
X12.58 Security Structures
X12.6 Application Control Structure
Information Processing Systems - Open Systems Interconnection - File Transfer, Acces and Management Part 1: General Introduction, ISO 8571/1
Security - Part 5 of the Open Systems Directive Version 1. X/Open Company Ltd, 1993.
IT - Sicherheitshandbuch. KBSt 1991.
Guide Defining and Buying Secure Open Systems. X/Open Company Ltd, 1992.
An Overview of CRAMM. CCTA 1992.
Útmutató az informatikai biztonsági szabályzat elkészítéséhez. ITB, Budapest, 1993.
Egyezmény az egyénnek a személyes adatok automatikus kezelésével kapcsolatos védelmérôl Európa Tanács, Strassburg, 1981. Informatika - Jog - Közigazgatás, Infofília I., Budapest, 1991.
Az OECD Tanács ajánlása a magánélet védelmét és a személyes adatok országhatárt átlépô áramlását szabályozó irányelvekre Gazdasági Együttmûködési és Fejlesztési Szervezet, Párizs 1981. Informatika - Jog - Közigazgatás, Infofília I., Budapest, 1991.
R (91) 10. sz. Ajánlás a közhivatalokban tárolt személyes adatok továbbításáról harmadik személynek Európa Tanács, Strassburg, 1991. Informatika - Jog - Közigazgatás, Infofília II., Budapest, 1991.
Az Európai Közösségek Bizottsága közleménye az egyénnek a személyes adatok kezelésével kapcsolatos védelmérôl és az információrendszerek biztonságáról Európai Közösségek Bizottsága, Brüsszel, 1990. Informatika - Jog - Közigazgatás, Infofília II., Budapest, 1991.
Az Informatikai Tárcaközi Bizottság 1. sz. ajánlása: "Kormányzati információtechnológiai fejlesztési keretprogram" (ITB 1992. VI.19.)

Az Informatikai Tárcaközi Bizottság 2. sz. ajánlása:"Az informatikai stratégia kialakításának és megvalósításának irányelvei" (ITB 1993. I. 13.)
Az Informatikai Tárcaközi Bizottság 3. sz. ajánlása: "Informatikai stratégiai tervezés a gyakorlatban" (ITB 1993. I.13.)
Az Informatikai Tárcaközi Bizottság 4. sz. ajánlása:"Az SSADM strukturált rendszerelemzési és tervezési módszer" (ITB 1993. I.13.)
Az Informatikai Tárcaközi Bizottság 5. sz. ajánlása:"Bevezetés a PRINCE projektirányítási módszertanba" (ITB 1993. I.13.)
Az Informatikai Tárcaközi Bizottság 6. sz. ajánlása:"Az X/OPEN specifikációnak megfelelô nyílt rendszerû termékek útmutatója" (ITB 1993. IX.14.)
Az Informatikai Tárcaközi Bizottság 7. sz. ajánlása:"Beszerzési ajánlások az X/OPEN XPG4 (XPG3) specifikációi és a GOSPI4 kormányzati OSI profil alapján" (ITB 1994. III.31.)

Forrás: http://www.itb.hu/ajanlasok/a8/html/a8_5.htm