Bugyi Önkormányzat Polgármesteri Hivatalának

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Hatályba lépés dátuma : 2015. június 01.

Tartalom jegyzék

Informatikai Biztonsági Szabályzat

A **Bugyi Önkormányzat Polgármesteri Hivatal** (a továbbiakban: Hivatal) Informatikai Biztonsági Szabályzatát, a továbbiakban IBSZ, a következők szerint határozom meg:

Az Informatikai Biztonsági Szabályzat az alábbi jogszabályokon alapul:

- a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról szóló módosított 1992. évi LXIII. törvény;
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló módosított 1992. évi LXVI. törvény;
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.

1. Az Informatikai Biztonsági Szabályzat célja

Az IBSZ alapvető célja, hogy az informatika alkalmazása során biztosítsa a Hivatalban az alábbiakat:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- munkaállomásokon lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését,
- a számítógépes rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit,
- a védelem működését a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen IBSZ a Hivatal adatvédelmének általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét. Szabályozza a számítástechnikai, informatikai eszközök használatának adatvédelmi biztonsági szabályait.

2. Műszaki alapfogalmak

- *szerver:* olyan hálózatra kapcsolt központi szerepet betöltő számítógép, amelynek alapvető feladata, hogy más, a hálózatra kapcsolt számítógépek vagy terminálok számára az erőforrásait megossza;
- *munkaállomás:* egy operátor vagy felhasználó számára, adott típusú feladathoz felszerelt számítógép vagy terminál;
- *szerverszoba:* nem légkondicionált helyiség, a Hivatal kijelölt dolgozói hozzáférhetnek a számítástechnikai eszközökhöz és szolgáltatásokhoz;
- *rack szekrény:* üvegezett, biztonságos fém szekrény, amelyben hálózati eszközöket, szervereket a szervertermen kívül üzemeltetnek;
- *adat:* a tények, az elképzelések nem értelmezett, de értelmezhető közlési formája;
- *adatállomány:* valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz;
- *adatbiztonság:* az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere;
- *adatfeldolgozás:* az adatok gyűjtése, rendszerezése, törlése, archiválása;

- *adatvédelem:* az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik;
- *alkalmazói program* (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be és amely a hardver és az üzemi rendszer funkcióit használja;
- *felhasználó:* az a személy vagy szervezet, aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához;
- *hardver:* az informatikai rendszer eszközeit, fizikai elemeit alkotó részei;
- *hálózat:* két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;
- *informatikai biztonság:* olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni;
- *rendszerprogram* (rendszer szoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

3. A Szabályzat hatálya

Az IBSZ **személyi hatálya** a Hivatal valamennyi köztisztviselőjére és a közhasznú foglalkoztatás keretében alkalmazottakra, illetve a számítástechnikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

Tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- az adatok felhasználására, tárolására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására,
- a Hivatal tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációra is,
- a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció),
- a rendszer- és felhasználói programokra.

4. Kapcsolódó szabályozások

Az IBSZ-t a Hivatal Szervezeti és Működési Szabályzatával és mellékleteivel, továbbá az adatvédelmi és adatbiztonsági szabályzattal összhangban kell alkalmazni.

5. Védelmet igénylő adatok, eszközök köre

A védelem tárgya:

- az alkalmazott hardver eszközök és azok működési biztonsága,
- a számítástechnikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk,
- az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszerszoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága,
- személyhez fűződő és vagyoni jogok,
- az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.

A védelem eszközei

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

6. A kiemelt védelem felelősei és tevékenységi köreik

Az informatikai biztonsági vezető

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a szervezet informatikai biztonsági vezetőjének kell gondoskodnia. Az adatvédelmi felelősi feladatok ellátásával megbízott személy kijelölését ezen szabályzat 1. számú melléklete tartalmazza.

Az informatikai biztonsági vezető feladatai :

- ellátja az adatfeldolgozás számítástechnikai felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- rendszeresen tájékoztatja a szervezet alkalmazottait a biztonsági helyzetben beállt esetleges változásokról,
- ellátja a számítástechnikai titokvédelmi munka szervezését és felügyeletét,
- a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával biztonságot növelő intézkedések kialakítása,
- felügyeli a számítástechnikai rendszerek üzembiztonságát, biztonsági másolatok, adatmentések készítését és karbantartását,
- a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos felügyelete,
- adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- adatvédelmi feladatok ismertetése,
- a védelmi rendszer érvényesülésének felügyelete,
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- ellenőrzi a vírusvédelem meglétét és használatát, frissítését
- tevékenységéről rendszeresen beszámol a Jegyzőnek.

Az informatikai biztonsági vezető ellenőri feladatai:

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- ellenőrzi a számítástechnikai munkafolyamat bármely részét előzetes bejelentési kötelezettség nélkül,
- adatvédelmi szempontból ellenőrzi az IBSZ naprakészségét, illetve azok végrehajtását.

Az informatikai biztonsági vezető jogai:

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Jegyzőnél,
- bármely érintett szervezeti egységnél jogosult informatikai tárgyú ellenőrzésre,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból a számítástechnikai beruházásokat véleményezi.

A hivatali informatikus feladatai:

Az informatikus feladatait a munkaköri leírása szerint látja el. Kiemelt feladatai:

- a védelmi rendszer érvényesülésének biztosítása,
- biztosítja a vírusvédelmi szoftver frissítését a szervezeti egységek számára,
- a szervezeti egységek kisebb számítógépes bázisainak üzemeltetése és az ehhez kapcsolódó számítástechnikai, adatvédelmi szolgáltatások biztosítása.

Védelmi feladata:

- biztosítja az üzemképességet és a műszaki ellátást, biztonsági másolatokat készít, gondoskodik a helyi adatok védelméről, mentéséről, tárolásáról;
- irányítja, segíti és ellenőrzi a munkatársak számítástechnikai munkáját;
- közreműködik a hardver és szoftver eszköz bázis fejlesztésében.

7 .1 Az IBSZ alkalmazásának módja

Az IBSZ megismerését az érintett köztisztviselők részére az adatvédelmi felelős biztosítja, az egyes munkaköri leírásoknak és az IBSZ előírásainak megfelelően.

Az IBSZ karbantartása

Az IBSZ-t a számítástechnikában, informatikában, valamint a Hivatalban bekövetkező változások miatt időközönként aktualizálni kell. Ez az adatvédelmi felelős feladata.

7.2 Értelmező rendelkezések

A szabályzat alkalmazása során:

7.2.1 adat: az információ megjelenési formája, azaz tények, elképzelések nem értelmezett, de értelmezhető közlési formája;

7.2.2 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;

7.2.3 különleges adat:

a) 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,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

7.2.4 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;

7.3 A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

1. közlésre szánt (bárki által megismerhető) adatok,
2. minősített adatok (titoknak minősülnek).

A számítógépes feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme hatáskörébe tartozik.

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

A kijelölt köztisztviselők előtt a titokvédelmi és egyéb rendszabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell. A titkot képező adatok védelmét, a feldolgozás - adattovábbítás,tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott titkosítással,illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftveres és hardveres adatvédelem).

8. Szervezeti egységek védelmi eszközei és módszerei

Általános rendelkezések

Tűzvédelem

A szerverszoba, szerverszoba a "D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a szerverszoba "Tűzvédelmi utasítás"-a tartalmazza, amely a Hivatal tűzvédelmi szabályzatának részét képezi.

Vagyonvédelem, fizikai biztonság

- a szerverszoba zárható,
- a szerverszobában csak a Hivatal kijelölt dolgozói végezhetnek munkát, az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők használhatják,
- a szerverszoba kulcsának felvétele és leadása csak aláírás ellenében a személyazonosság igazolása mellett történhet,
- munkaidőn túl a szerverszobába csak engedéllyel lehet tartózkodni,
- a szerverszobába történő illetéktelen behatolás tényét a szervezet vezetőjének azonnal jelenteni kell,
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Adathordozók védelme, tárolása, hordozása és karbantartása

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni,
- a használni kívánt adathordozót (floppy disk, CD-ROM, stb.) a tárolásra kijelölt helyről kell kivenni és oda kell vissza is helyezni,
- az adathordozók szállítása csak megfelelő módon történhet,
- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozás'hoz szükségesek,
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével lehet,
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg,
- az adathordozókat félévenként ellenőrizni és tisztítani kell,
- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő:
    a. a fizikailag sérült, javíthatatlan,
    b. a gyári, raktározási hibából követően felhasználásra alkalmatlan (deformálódott),
    c. ha a kapacitás a névleges érték 75%-ánál kevesebb,
    d. véglegesen elhasználódott adathordozót,

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni, bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést az Egyedi Iratkezelési Szabályzatnak megfelelően kell lefolytatni. S okszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni, az üzemi másolás nem minősül másolásnak, biztonsági illetve archív adatállomány előállítása másolásnak számít.

Az adathordozókat az Egyedi Iratkezelési Szabályzatnak megfelelően kell leltározni. *Adatvédelemi feladatok:*

- az adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- csak tesztelt adathordozóra lehet adatállományt rögzíteni,
- adatrögzítés szoftver védelme: a programokat és az adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni,
- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen hozzáférési szinten férhet hozzá a programokhoz és 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.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adattárolókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

Vírusvédelem

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani. Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a szervezeti egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

Szoftverek beszerzése

Bármely új szoftver csak az illetékes irodavezető javaslatával az informatikus véleményével igényelhető és a hivatal vezetőjének engedélyével szerezhető be, a kötelezettségvállalásra vonatkozó szabályok figyelembevételével.

Tilos bármely ismeretlen, azonosítatlan, vagy a Polgármesteri Hivatal tevékenységi körébe nem tartozó szoftver vagy adatbázis telepítése, használata. Általános és kötelező érvényű szabály az, hogy a munkahelyi számítógépek csak munkahelyi kiemelt célokra használhatók.

Az ismeretlen azonosítatlan szoftverek kiszűrése és a használatának megszüntetése érdekében az informatikus köteles dokumentált módon a szervert havonta a munkahelyi gépeket pedig évente e tekintetben ellenőrizni. Az informatikus ellenőrzési kötelezettsége a mellett a helyi és hálózati adattárolókra való adatmásolásért mindenki személyes felelősséggel tartozik különös tekintettel a saját gép winchester tartalmára.

Szoftver védelem

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

- Rendszerszoftver védelem:
  a) a rendszerszoftver módosításához az adatvédelmi felelős engedélye szükséges,
  b) a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni,
  c) a rendszerszoftver-eseményekről és a változtatásokról feljegyzést kell készíteni.

- Programhoz való hozzáférés, programvédelem:

A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

- A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:
  a) a program azonosítója,
  b) a program készítőjének neve,
  c) a feldolgozási rendszer megnevezése.

- Programok megőrzése, nyilvántartása:
  a) a programokról naprakész nyilvántartást kell vezetni,
  b) a nyilvántartásból egyértelműen megállapíthatóak legyenek a program azonosítására és kezelésére vonatkozó adatok.

- Programok fizikai védelme:A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni.

Szakmai programok

Hivatalunk elektronikusan tárolt hatályos jogszabály gyűjteményt alkalmaz (továbbiakban CD Jogtár). Biztosítani kell minden irodában a CD Jogtárhoz való hozzáférést. Az egyes irodák által használt szakmai programok hozzáférési lehetőségét a 2. sz. melléklet tartalmazza.

Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől,
- a számítógép közelében ételt és italt fogyasztani tilos,
- a szerverszobában klímaberendezés használata ajánlott,
- szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben a szerverszobában kell elhelyezni,
- a számítógép-hálózat csatornáit lehetőleg külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát,
- a fali csatlakozók megbontása szigorúan tilos,
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez,
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni,
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az informatikus, illetve a szervizek szakemberei nyúlhatnak bele,
- havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.

A hálózati jogosultságok, jelszavak, adatbiztonság

A tárolt adatok elérésének szabályozása érdekében az informatikus kötelessége a felhasználónak belépési név, jelszó, valamint a feladat elvégzéséhez és csak az ahhoz szükséges hálózati jogosultság definiálása. Azáltal, hogy a felhasználók csak meghatározott lemezterületekre írhatnak, csak az általuk szükséges programokat használhatják s az ezeknez szükséges jelszavakat ismerik: egyrészt az illegális szoftver másolás korlátozható, másrészt a munkakörébe nem tartozó adatokhoz, programokhoz való hozzáférés korlátozott. A Polgármesteri Hivatal tevékenységi körében tartozó felhasználói programokhoz, azok egyes funkcióihoz való hozzáférési jogosultságok kialakítása az illetékes irodavezető és az informatikus közös feladata. A számítógépek kezelői kötelesek a jelszavakat titkosan kezelni, szükség esetén a jelszavakat is a biztonság érdekében megváltoztatni. Az adatbiztonság további eleme az adatok megsemmisülése, illetve sérülése elleni védekezés. Az informatikus feladata megfelelő mentési eljárások elkészítése, a kijelölt felhasználók pedig kötelesek a meghatározott időközökben a mentést elvégezni. A mentések során felmerült problémákról az informatikust tájékoztatni kell. A mentések rendjét az 5. sz. melléklet tartalmazza.

Személyzeti felvétel /kiléptetés rendje

Személyi felvétel esetén a szervezet megbízott informatikai biztonsági vezetője az új dolgozóval ismerteti a szervezet biztonsági szabályzatát , utasítást ad a rendszergazdának az adott munkahely , és a munkaállomáson futó programok jelszavának átadására . Az új munkatárs a biztonsági szabályzat elfogadását, és a jelszavak átvételét aláírásával igazolja.

Személyi kiléptetés esetén a rendszergazda a kilépő munkatárstól bevonja a kint lévő jelszavakat /biztonsági kulcsokat , és új jelszavak generálásával hozzáférhetetlenné teszi számára a szervezet informatikai rendszerét adat állományát. Amennyiben az érintett adatok jelege azt megkívánja a munkaügyi osztály titoktartási jegyzőkönyvet készít , és a kilépő munkatárssal azt aláíratja.

Internetes elérés, elektronikus levelezés

Az internet elérés teljes mértékben kábelnet és Wi-Fi kapcsolaton keresztül valósul meg. A kábelnet és Wi-Fi kapcsolat lehetővé teszi az üzembe helyezett szerver kommunikációját, valamint az internet elérésen kívül az elektronikus levelezést is. Az internet elérés a hivatal minden irodájában teljes körűen biztosított. Az általános hivatali email cím Szatmari.Attila@bugyi.hu, az így beérkezett levelek nyomtatott formában kerülnek érkeztetésre, majd az Egyedei Iratkezelési Szabályzat szerint kell eljárni.

GIRO átutalás

Az ügyfélterminál rendszer a Polgármesteri Hivatal Pénzügyi osztályán működik. Különleges jogosultsági és biztonsági rendszer használata szükséges a működéshez. Ügyfélterminálon keresztül történik a számlák kiegyenlítése. Csoport átutalással történik a munkabér, bérjellegű juttatások, a szociális ellátásról, gyermekek védelméről törvényben szabályozott ellátások utalása.

A számlatulajdonos előállítja az utalási megbízásai számítógépes tételeit az ügyfélterminál rendszerben való adatrögzítéssel és/vagy saját informatikai rendszeréből történő áttöltéssel a felhasználói leírás minőségi feltételeinek megfelelő floppy lemez adathordozón, adattartalommal és formai előírások szerint. Ezt követően a számlatulajdonos ügyintézője titkos jelszó (PIN-kód) alkalmazásával megküldi azokat az OTP Bank Zrt. részére az ügyfélterminálon keresztül. A rendszerben az aláíró a OTP Bank Zrt-nél az aláírási címpéldány szerint bejelentettek.

Hardver beszerzés, szerverek munkahelyek konfigurálása

Az informatikai eszközök fejlesztésének forrása az önkormányzat éves költségvetésébe kerül betervezésre. A beruházási tervnek megfelelően - a Polgármesteri Hivatal vezetőségének jóváhagyását követően - az informatikus feladata a szerver és az egyes irodákban lévő számítógépes konfigurációk, alkatrészek, szoftverek beszerzése. A beszerzések a Közbeszerzési Szabályzatban meghatározott módon kell elvégezni. Nyilvántartott munkahelyi konfigurációkat átalakítani, alkatrészeket cserélni, csak a belső szabályzásnak megfelelően, kizárólag az informatikus tudomásával és a gazdálkodási iroda által vezetett nyilvántartás módosításával lehet.

A Hivatal további védelmi előírásai

A védelem felelőse a Jegyző.

Biztonsági osztály , és biztonsági szint meghatározása:

Az információbiztonságáról szóló 2013.évi L. törvény 77/2013. (XII. 19.) NFM rendelete 1. § értelmében Bugyi Polgármesteri Hivatal rendszerét 2-es biztonsági osztályba sorolom.

Az információbiztonságáról szóló 2013.évi L. törvény 77/2013. (XII. 19.) NFM rendelete 1. § értelmében Bugyi Polgármesteri Hivatal rendszerét 2-es biztonsági szintben határozom meg.

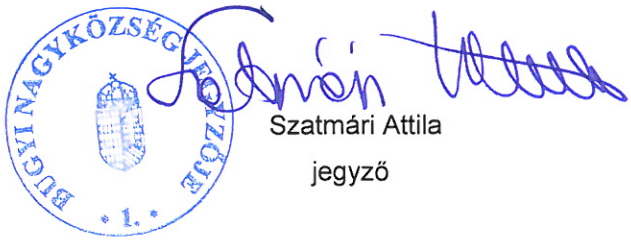
Védelmi előírások:

- a számítógépeket csak indítójelszóval lehessen elindítani,
- induláskor minden esetben vírus-ellenőrző programot kell elindítani,
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell,
- mindkét esetben a jelszóknak különbözőknek kell lenniük
- a bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel, vagy külső programmal is,
- a módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni,
- a teljes anyagról heti mentéseket kell készíteni, ezeket a havi mentésekig kell megőrizni,
- a teljes anyagról havi mentéseket kell készíteni, ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény),
- a felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól külön, tűzbiztos helyen kell tárolni.

9. Hatályba léptetés

Ezen szabályzat 2015. június 01 napon lép hatályba.

Kelt: Bugyi, 2015. június 01.



Szatmári Attila

jegyző

Az informatikai biztonsági vezető kijelölése

A szabályzat 6.1. pontja alapján az informatikai biztonsági vezető feladatainak ellátásával megbízott személy :

- Neve: Szivósné Nagy Szilvia
- Végzetsége : BKÁE Államigazgatási Kar : Településmenedzser
- Munkáltató megnevezése : Bugyi, Polgármesteri Hivatal

Kelt: Bugyi , 2015. június 01.

BUGYI NAGYKÖZSÉG JEGYZŐJE * 1. *

Szatmári Attila
Jegyző

Záradék: az adatvédelmi feladatok ellátásra való kijelölést tudomásul veszem, az IBSZ-t és az abban foglaltakat megismertem és magamra nézve kötelezőnek ismerem el.

Kelt: Bugyi , 2015. június 01.

Szivósné Nagy Szilvia
Informatikai biztonsági vezető

Szerverszoba rend

1. A szerverszobában a Hivatal köztisztviselőin kívül más nem tartózkodhat. Más személyek benntartózkodását a szervezeti egység vezető engedélyezheti.

2. Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát csak a nyilvántartásban szereplő személyek kaphatják meg. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a szerverszobában.

3. A szerverszobában az esztétikus, higiénikus, folyamatos munkavégzés feltételeit kell megőrizni. A szerverszobában rend megtartásáért és a biztonságos műszaki üzemeltetésért az informatikus a felelős.

4. A szerverszobába égő cigarettával belépni, és ott dohányozni valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!

5. A szerverszoba takarítását csak az arra előzőleg kioktatott személyek végezhetik.

6. A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak az informatikus és a szervizek szakemberei végezhetnek.

7. A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni.

8. A szerverszobában elhelyezett adathordozókat csak az informatikus engedélyével lehet használni.

9. Adathordozókat csak az informatikus engedélyével lehet be- és kivinni a szerverszobából.

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

11. A szerverszobába el kell helyezni jelzőberendezéseket (klíma, tűz- és betörésjelző), melyeknek műszaki állapotát folyamatosan figyelni kell az ott dolgozóknak és bármilyen rendellenességet azonnal jelenteni kell a munkavédelmi ügyintézőnek.

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

A fenti rendelkezések megsértése esetén az elkövetővel szemben az adatvédelmi felelős fegyelmi felelősségre vonást kezdeményezhet.

Átvételi jegyzék

A Bugyi Önkormányzat Polgármesteri Hivatala 2015. június 01.-től hatályos informatikai biztonsági szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartatni.

Név	Feladat, hatáskör	Dátum	Aláírás
Somogyi Béla	polgármester	2015.07.01	
Nagy András Gábor	alpolgármester	2015.07.01	
Szatmári Attila	jegyző	2015.07.01	
Szivósné Nagy Szilvia	igazgatási csoportvezető	2015.07.01	
Virág Károlyné	igazgatási ügyintéző	2015.07.01	
Harangozó Andrásné	igazgatási ügyintéző	2015.07.01	
Juhász Judit	igazgatási ügyintéző	2015.07.01	
Kiss Jánosné	igazgatási ügyintéző	2015.07.01	
Török Edina	igazgatási ügyintéző	2015.07.01	
Mészáros Ernő	műszaki ügyintéző	2015.07.01	
Pótiné Safranyik Anikó	pénzügyi vezető	2015.07.01	
Parlaginé Pirityi Ildikó	pénzügyi ügyintéző	2015.07.01	
Sutiné Deák Ildikó	pénzügyi ügyintéző	2015.07.01	
Nagyné Boros Andrea	pénzügyi ügyintéző	2015.07.01	
Gál Andrea	pénzügyi ügyintéző	2015.07.01	
Majsai Katalin	adóügy	2015.07.01	
Szadai Pálné	adóügy	2015.07.01	
Krizsán Ferencné	hagyaték ügyek	2015.07.01	
Stengl Tamásné	anyakönyv-állampolg. ügyek	2015.07.01	
Bai Miklósné	település rendezés	2015.07.01	
Földvári Imréné	közterület ügyintézés	2015.07.01	

4. számú melléklet

Jogosultságok programokhoz beosztás alapján

Programok		ONKADO	Önkormányzati portál rendszer	Iktatórendszer	ELEKTRA Elektronikus pénzügyi rendszer	CT-ECOSTAT	Népesség-nyilvántartó program (Helyi Vizuál Regiszter)	Illetmény számfejtő rendszer, intézményi modul (K,I.R,3)	Takarnet - Földhivatali Információs Rendszer	Telepinfo és Kerinfo	Mezőőri hozzájárulás befizetését nyilvántartó Program
Szatmári Attila	jegyző	X	TH	X	TH	X	X	X	X	X	X
Pótiné Safranyik Anikó	mb. pénzügyi vezető	X	TH	X	TH	TH	X	X	X	X	X
Sutiné Deák Ildikó	pénzügyi előadó	X	MO	X	TH	TH	X	X	X	X	X
Boros Andrea	pénzügyi előadó	X	MO	X	MO	TH	X	TH	X	X	X
Parlaginé Pirityi Ildikó	pénzügyi előadó	X	MO	X	MO	TH	X	X	X	X	X
Gál Andrea	pénzügyi előadó	X	MO	X	MO	TH	X	X	X	X	TH
Krizsán Ferencné	igazgatási előadó	X	MO	X	X	X	X	X	X	X	X
Stengl Tamásné	igazgatási előadó	X	MO	X	X	X	TH	X	X	TH	X
Majsai Katalin	pénzügyi előadó - adó	TH	MO	X	MO	X	X	X	X	X	X
Szadai Pálné	pénzügyi előadó - adó	TH	MO	X	X	X	X	X	X	X	X
Harangozó Andrásné	igazgatási előadó	X	MO	TH	X	X	X	TH	X	X	X
Virág Károlyné	igazgatási előadó	X	MO	TH	X	X	X	X	X	X	X
Mészáros Ernő	műszaki előadó	X	MO	X	X	TH	X	X	TH	X	X
Török Edina	igazgatási előadó	X	MO	X	X	X	X	X	X	X	X
Juhász Judit	igazgatási előadó	X	MO	X	X	X	X	X	X	X	X
Földvári Imréné	közterületfelügyelő	X	MO	X	X	X	X	X	X	X	X
Somogyi Béla	polgármester	X	TH	X	TH	X	X	X	X	X	X
Nagy András Gábor	alpolgármester	X	TH	X	TH	X	X	X	X	X	X
Szivósné Nagy Szilvia	igazgatási csoportvezető	X	TH	X	TH	X	X	X	X	X	X

Megtekintésre : M

Módosítás : MO

Teljes hozzáférés : TH
Nincs Hozzáférés : X

Bugyi Polgármesteri Hivatal adatmentési rendje

Program	Iroda	Mentés gyakorisága	Honnan	Hová	Felelős
Bugyi Polgármesteri Hivatal					
ÖNKORMÁNYZATI PORTÁL REND.	Igazgatási iroda	naponta	Szerver adatbázis	C:\ és Szerverre	*Szivósné Nagy Szilvia*
VIZUAL REGISZTER	Igazgatási iroda	naponta	C:\Inventory	C:\Inventory /USB	*Stengl Tamásné*
CT-ECOSTAT	Pénzügyi iroda	adatbevitelkor, naponta, havonta	Szerver adatbázis	C:\ és Szerverre	*Pótiné Safranyik Anikó*
KIR3	Gazdasági iroda	fogadás előtt és után, esetenként, számfejtéskor, nyilvántartás szerint	C:\Inventory	C:\Inventory /USB	*Harangozó Andrásné*
IKTATÓ RENDSZER	Igazgatási iroda	adatbevitelkor	C:\	C:\Inventory /USB	*Harangozó Andrásné*
ELEKTRA	Pénzügyi iroda	adatbevitelkor	C:\	C:\Inventory /USB	*Pótiné Safranyik Anikó*
ÖNK. ADO	Igazgatási iroda	adatbevitelkor	C:\	C:\Inventory /USB	*Majsai Katalin*
TAKAR- NET	Igazgatási iroda	adatbevitelkor	C:\	C:\Inventory /USB	*Mészáros Ernő*
TELEPINFO és KERINFO	Igazgatási iroda	naponta	C:\	C:\Inventory /USB	*Stengl Tamásné*
MEZŐŐRI H.B. NYILVÁNTARTÓ	Pénzügyi iroda	naponta	C:\	C:\Inventory /USB	*Gál Andrea*