GYŐRÚJFALU KÖZÖS ÖNKORMÁNYZATI HIVATAL VÁMOSSZABADI KIRENDELTSÉGE

INFORMATIKAI BIZTONSÁGPOLITIKÁJA

IBP dokumentum karbantartás

verzió	kiadás	módosítás leírás	készítő módosító (IBF)	elfogadás	elfogadás
1.0	2014.10.30	Alap verzió			
1.01	2016.11.15	Felülvizsgálat			

2. Vezetői összefoglaló és bevezetés

A **Győrújfalu Közös Önkormányzati Hivatal Vámosszabadi Kirendeltsége** (továbbiakban Hivatal) vezetésének szilárd meggyőződése, hogy a, az információ a Hivatal és az állampolgárok olyan vagyona, amelyet védeni kell a különböző fenyegetések ellen, a bizalmasság, a sértetlenség és a rendelkezésre állás, illetve az üzletmenet folytonosságának biztosítása érdekében.

Ennek elérésére a Hivatal legfelső vezetése a mindenkori Informatikai **Biztonsági Stratégiát szem előtt** tartva a jelen **Információ Biztonsági Politikában** (a továbbiakban IBP) meghatározott egyetemleges alapelvek és belső biztonsági alapkövetelmények maradéktalan teljesítését várja el a vezetőktől, valamennyi munkatársától, beszállítótól és minden egyéb közreműködőtől.

A Hivatal informatikai biztonságpolitikája kivétel nélkül kiterjed a Hivatal által végzett valamennyi folyamatra és valamennyi szervezeti egységre.

A vezetés biztosítja a teljesítéshez alapvetően szükséges erőforrásokat.

3. A politika célja

Az IBP a Hivatal vezetésének akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzésére és fenntartására irányuló intézkedések bevezetésére. Az IBP alapul szolgál a politikánál alacsonyabb szintű szabályozás, kialakítására és bevezetésére.

Az információ védelem megvalósítása érdekében tervezni és biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő irányvonal technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

4. Általános rendelkezések

4.1 Az IBP hatálya

4.1.1 Személyi hatály

Az IBP személyi hatálya kiteljed azon

- a Hivatal minden munkatársára,
- a Hivatal informatikai üzemeltetést végző, kiszervezett tevékenységeit ellátó (külső) partnereire,
- a Hivatal informatikai üzemeltetését és/vagy fejlesztését végző, illetve egyéb szerződéses viszonyban tevékenykedő partnereire.

A jelen Szabályzat személyi hatálya alá tartozóknak a politika célkitűzéseit ismerniük és követniük kell.

4.1.2 Tárgyi hatálya

Az IBP Tárgyi hatálya kiterjed az Hivatal

- adathordozóira,
- alkalmazásaira,
- alapszoftvereire,ü
- hardver elemeire,
- környezeti infrastruktúra elemeire,
- objektumaira.

4.1.3 Területi hatálya

Az IBP területi hatálya kiterjed a Tárgyi hatálya alá tartozó informatikai erőforrások üzemelési és használati helységeire:

- a Hivatal telephelyére
- mindenkori bérelt helyiségeire
- a személyes (otthoni) használatra adott eszközökre.

4.2 Az Informatikai Biztonságpolitika minősítése

Az IBP nyilvános dokumentum. Az IBP nyilvánosság számára történő elérhetőségét az Hivatal honlapján nyilvánosan elérhetővé teszi.

4.3 Elhelyezkedése, megfelelősége

Az IBP a Szabályozási hierarchia legfelsőbb szintjén helyezkedik el és ilyen módon hatással van a teljes Szabályozási struktúrára.

Ismerete és betartása minden munkatársra kötelező érvényű. Az Információ Biztonsági Politika, majd az erre épülő Informatikai Biztonsági Stratégia és Informatikai Biztonsági Szabályzat kibocsátása, az érintettek körében történő közzététele a Hivatal Jegyzőjének, karbantartatása és folyamatos felülvizsgáltatása az Informatikai biztonsági felelős feladata.

A jelen IBP-ben megfogalmazottak megfelelnek a hazai jogszabályoknak.

4.3.1 Felülvizsgálat

Az IBP rendszeres felülvizsgálata alapvető fontosságú elvárás. Az IBP-t a törvényi, környezeti és jelentős feladat változás esetén, de legalább két évente felül kell vizsgálni, a felülvizsgálat az Informatikai Biztonsági Felelős (IB Felelős) feladata.

4.3.2 Kommunikáció

Az IBP-t a Hivatal minden munkatársának ismernie kell, kiemelten azoknak, akik az Hivatal informatikai rendszerét használják és üzemeltetik. Ez utóbbi esetben az IBP megismerését és tudomásul vételét dokumentálni kell.

5. Informatikai Biztonságpolitikai alapelvek és célkitűzések

A Hivatal az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánja következetesen érvényesíteni a jogszabályi követelményeknek és Felügyeleti elvárásoknak megfelelően.

5.1 Alapelvek

Az informatikai rendszerekben adatot, információt és egyéb szellemi tulajdont az intézmény számára felmérhető, értékével arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a sérüléstől, megsemmisüléstől és a nyilvánosságra kerüléstől. A védelemnek biztosítani kell az informatikai rendszer megbízható működését fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén. A biztonsági szabályok megsértése esetén az IBP hatálya alá eső személyekkel szemben felelősségre vonási eljárást kell kezdeményezni.

A védelem teljes körűségének alapelve

A teljes körűségre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:

a) az összes rendszerelemre,

b) a rendszerek architektúrájának minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az alkalmazások szintjén,

c) mind a központi, mind a végponti informatikai eszközökre és környezetükre.

A védelem zártságának alapelve

A zárt védelem akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések megvalósításra kerültek, és azok szerves egységet alkotnak.

A védelem kockázat arányosságának alapelve

A védelem mértéke és költségei a felmért kockázatokkal arányos legyen. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.

A védelem folytonosságának alapelve

Az informatikai rendszerek bevezetése során kialakított védelmi képességeket a rendszer teljes életciklusa alatt folytonosan biztosítani és fejleszteni kell.

5.2 Célkitűzések

Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk vonatkozásában, hogy minden kétséget kizáróan megállapítható legyen a bekerülő adat forrása és az adat valóságnak való megfelelőssége, valamint annak biztosítása, hogy az előállítás után megőrizze ezen minőségét, azaz:.

Bizalmasság biztosítása a Hivatal által kezelt adatokhoz való hozzáférés tekintetében. Érvényesülését elsősorban az informatikai rendszerben történő adathozzáférések és adatkezelés, valamint a Hivatal kommunikációja során kell biztosítani.

Sértetlenség biztosítása a Hivatal adatkezelése, adatfeldolgozása és kommunikációja során.

A Hivatal által történő adatkezelés során követelmény, hogy pontos és a valóságnak mindenben megfelelő információk kerüljenek a rendszerben feldolgozásra, és ezen információ sértetlensége az adatkezelés sorén mindvégig biztosított legyen.

Rendelkezésre állás biztosítása a Hivatal által kezelt adatok tekintetében.

A feldolgozott információ tekintetében követelmény annak visszakereshetősége, melynek záloga az informatikai rendszerek funkcióinak és elérhetőségének folyamatos biztosítása. Működőképesség fenntartása az Önkormányzat és szervei informatikai rendszereire és rendszerelemeire vonatkozóan, amely az adott informatikai eszköz vagy rendszer elvárt és igényelt üzemelési állapotban való fennmaradását jelenti. Ennek elérése céljából biztosítani kell a megfelelően képzett személyzetet és technikai feltételeket

6. Kockázatalapú megközelítés

A Hivatal vezetése célul tűzte ki hogy

– a kockázatokkal arányos védelem biztosítása érdekében

– kockázatelemzés rendszeres, belső szabályozás szerinti elvégzését a fenyegetések, a gyenge pontok, a nem elviselhető kockázati tényezők meghatározására,

- valamint az ezek alapján kialakítandó védelmi intézkedéseket, melyekhez felelőst és határidőt kell rendelni.

6.1 Kockázati tényezők

A Hivatal számára az információbiztonság sikeres megvalósítása során kritikus tényezők a következők:

- a vezetőség elkötelezettségének mértéke;

- a környezet naprakész és pontos meghatározása a biztonsági szabályozáshoz
- a biztonsági követelmények, a kockázatbecslés és a kockázatkezelés megértése és helyes alkalmazása;
- a biztonság hatékony menedzselése valamennyi érintett felé;
- gondoskodás a kellő oktatásról és képzésről;
- átfogó, mindenre kiterjedő és kiegyensúlyozott ellenőrzési rendszer bevezetése, a teljesítőképességének értékeléséhez és a helyesbítési javaslatok visszacsatolásához.
- a biztonsági események kezelésének megfelelő szabályozása, értékelése, visszacsatolása

7. Szervezeti és felelősségi kérdések

A Hivatal vezetője köteles gondoskodni az elektronikus információs rendszerek védel-méről a 2013.évi L. törvényben meghatározottak szerint.
Az IBP-ben lefektetett elvek kidolgozásának és betartatásának Hivatalon belül, minden esetben kell, hogy legyen felelőse.
Az Információ Biztonsági Felelős – IB Felelős közvetlen a Jegyzőhöz rendelt pozíció vagy megbízott esetén vele közvetlen kapcsolatban lévő kell hogy legyen. AZ IBP elvek betartásának helyzetéről az IB Felelős rendszeresen beszámol a Jegyzőnek, aki az információ biztonsági feladatok megvalósításának feltételeit biztosítja.
IBP betartása minden munkatárs feladata és annak be nem tartása szankciókat von maga után.

8. Adminisztratív védelem és intézkedések

Az informatikai rendszerben bekövetkezett változásokat az alkalmazott nyilvántartásokat, és a problémakezelést dokumentált formában, a szabályozó előírásoknak megfelelően kell végezni.
Az informatikai biztonsági dokumentációs rendszer aktualitásának fenntartása érdekében a rendszerben található dokumentumok rendszeres karbantartást igényelnek.
A dokumentációs rendszer dokumentumait felül kell vizsgálni a következő változások esetekben:

- a törvényi előírások vagy az irányító hatóság rendelkezési új helyzetet teremtenek
- a szervezet igényei, céljai megváltoznak,
- új területek, szolgáltatások jelennek meg,
- informatikai szolgáltatások szűnnek meg,
- új informatikai technológiák kerülnek bevezetése,
- informatikai technológiák alkalmazása szűnik meg,
- a kockázatelemzés következtében új, lényeges változtatások válnak szükségszerűvé.

Az adminisztrációs biztonság területén az Hivatal vezetésének célkitűzései az alábbiak:

- az Hivatal folyamatos, zavartalan és hatékony működését biztosító informatikai szabályozókörnyezet, illetve feltételrendszer megteremtése,
- a szabályozás érinti a kockázat kezelés szabályozását, ügymenet folytonosságot, a biztonsági események kezelését, az emberi tényezőket, és a tudatosság fokozását
- a kialakított rendszer ellenőrzése és a visszacsatolással folyamatos tökéletesítése

9. Fizikai védelem

A Fizikai és szervezeti biztonság, környezeti infrastruktúra területén a Hivatal vezetésének célkitűzései az alábbiak:

- a Hivatal objektumának, szervezetének biztonságának szavatolása, az információ kezelését, feldolgozását végző helyiségek, valamint az egyes eszközök, az abban elhelyezett adattárolók és adathordozók fizikai védelmének biztosítása,
- papír formában, valamint elektronikusan kezelt és tárolt információk, tárgyi eszközök, vagy szolgáltatást végző személyek védelmének biztosítása a különböző eseményektől, mint tűz, víz, áramellátás kimaradása, külső támadások, betérés,
- informatikai, vagy egyéb úton keletkezett adatok és információk kezelése során az előírt fizikai informatikai biztonsági követelmények betartásának elősegítése,
- szállításra, karbantartásra vonatkozó fokozott biztonsági intézkedések bevezetése
- személyi felelősségek egyértelmű meghatározása és elhatárolása.

10. Logikai védelem

A logikai biztonság területén a Hivatal vezetésének célkitűzései az alábbiak:

- informatikai rendszerek védelmének megteremtése a jogosulatlan hozzáférésektől,
- az informatikai rendszerekhez és alkalmazásokhoz való hozzáférési jogok engedélyezésének hivatalos eljárások keretében történő szabályozása,
- információ, illetve adatvagyon megfelelő védelmi szintjének kialakítása, valamint az információ osztályozása az adatvédelmi szabályzattal összhangban,
- rosszindulatú szoftverek:
    - számítógépvírusok, a hálózati férgek, a trójai falovak és a logikai bombák elleni védekezés hatékony kialakítása,
    - az A Hivatal kiemelt figyelmet fordít a felhasználói szoftverek jogtisztaságára, mindent megtesz a jogtiszta szoftver használat érdekében és az illegális használat, illetve másolás ellen

  - Internet használat és elektronikus levelezés létesítése és üzemeltetése vonatkozásában megfelelő tűzfalas védelem kialakítása a külső támadások, illetve a belső erőforrásokhoz történő jogtalan külső hozzáférések megakadályozására,
- biztonsági követelmények érvényesítése minden, a Hivatal külső informatikai adat-, vagy számítástechnika kapcsolatában, az ennek kialakítására irányuló szerződésekben, vagy megállapodásokban,
- jogosulatlan tevékenységek észlelésének megteremtése,
- adathordozók védelme, adattárolás, mentés, karbantartás szabályozása
- informatikai biztonság megteremtése a mobil számítástechnikai eszközök (távmunka) használata esetén. A megkívánt biztonság legyen összemérhető azzal a kockázattal, amelyet ez a lehetőség hordoz,
- mentési rendszer kidolgozása, bevezetése
- rendkívüli események kezelésére történő eljárásrend bevezetése,
- alaptevékenységek megszakadásának kezelése, és a kritikus szolgálati folyamatok megvédése a nagyobb meghibásodások és a katasztrófák hatásaitól.

11. Információ Biztonsági események kezelése

A Hivatal célul tűzte ki, a kockázatokkal arányos védelem biztosítása érdekében a kockázatelemzés alapján kialakított szabályozott eseménykezelést, az incidensek elkerülésére. Az eljárásban meghatározza az eseménykezelés folyamatát az egyes szerepköröket és feladataikat, az eljárás dokumentálását. Az eljárás lezárásával dokumentálni kell az intézkedéseket, a felelősségi kérdéseket

12. Az információ biztonság ellenőrzése, fenntartása

Az IBP által megkövetelt információ biztonsági irányítási rendszer fenntartása alapvetően fontos stratégia cél. Ennek felelőse az IB Felelős. Az IB Felelős által elvégzendő távlati feladatokat az Informatikai Biztonsági Stratégia, az IB Felelős rendszeres feladatait pedig az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) tartalmazza. A stratégiában elhatározott és az IBSZ-ben előírt feladatok végrehajtásához szükséges feltételek biztosításáért a Jegyző felel.

A Hivatal biztonságirányítási rendszerének fenntartásához elengedhetetlenül szükséges a munkatársak biztonságtudatosságának fejlesztése és fenntartása. Ennek érdekében kell végrehajtani és dokumentálni a munkatársak évenkénti biztonsági oktatását.

13. Az információ biztonság szintjei

Az informatikai biztonság szintbe és osztályba sorolást a 2013. évi L törvény szerint kell elvégezni.

Meg kell állapítani a Hivatal szervezetének biztonsági szintjét, az Ibtv. 9. § szerint a 41/2015. (VII. 15.) BM (Kövr.) rendeletbe foglaltaknak megfelelően**.** Az elektronikus információs rendszereket a Kövr. szerinti feltételekkel biztonsági osztályba kell sorolni.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg.

A biztonsági szintbe sorolásnál a Hivatalt egy szervezetként kezeljük, míg az osztályba sorolásnál az alkalmazásokat hasonló tulajdonságaik alapján egyként dokumentáljuk.

A szervezet biztonsági szintje 1-5-ig terjedően kerül besorolásra.

Az egyes biztonsági osztályok meghatározása 1-5-ig terjed a kezelt adatok, a káresemény nagysága, a bizalomvesztés mértéke, a közvetlen és közvetett anyagi kár figyelembe vételével.
A biztonsági osztályba sorolást a szervezet vezetője a Hivatalvezető hagyja jóvá és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért.
A megállapított biztonsági szint és osztály az IBSZ-ben kerül rögzítésre. Amennyiben az elvárt és aktuálisan megállapított szint között eltérés van cselekvési terv készül a védelmi intézkedések megtételére, a felelősök és a javasolt határidők meghatározásával.

6. Fogalmak és meghatározások

Az IBP-ben használt fogalmak és meghatározások értelmezése a 2013 évi L térvény fogalmaival és definícióival azonosak.