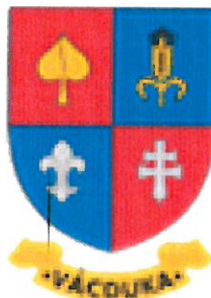


VÁCDUKAI KÖZÖS ÖNKORMÁNYZATI HIVATAL

B06 INFORMATIKAI BIZTONSÁGI POLITIKÁJA (IBP) V1.0





Tartalomjegyzék

1	BEVEZETÉS	3
1.1	Az Informatikai Biztonsági Politika célja	3
1.1.1	Az információbiztonság keretrendszere	3
1.1.2	Az információbiztonság aspektusai	3
1.2	Jóváhagyás	4
1.3	Az Informatikai Biztonsági Politika felülvizsgálta	4
1.4	Az Informatikai Biztonsági Politika értékelése	4
1.5	Az Informatikai Biztonsági Politika hatálya	4
1.5.1	Az ITBP alanyi hatálya	5
1.5.2	Az ITBP tárgyi hatálya	5
1.5.3	Az ITBP időbeli hatálya	5
	Az ITBP időbeli hatálya visszavonásig érvényes.	5
1.6	Informatikai biztonsági felelős	5
1.7	Vezetőségi elkötelezettség	5
1.8	Kapcsolódó dokumentumok	5
2	A KOCKÁZATELEMZÉS ALAPELVEI	5
3	AZ OSZTÁLYBA SOROLÁS ALAPELVEI	5
4	AZ INFORMATIKAI BIZTONSÁG ALAPELVEI	6
4.1	A kockázatarányos védelem elve	6
4.2	Teljes körű védelem elve	6
4.3	Az egyenszilárdság elve	6
4.4	Rendszerfejlesztések biztonsági elv	6
4.5	A „négy szem” elv	6
4.6	A szükséges és elégséges hozzáférés elve	6
4.7	Fizikai biztonság	6
4.8	Vírusvédelem	6
4.9	Mentés, archiválás	7
4.10	Naplózás	7
4.11	Incidensek kezelése	7
4.12	Működésfolytonosság fenntartása	7
4.13	Oktatás, képzés, - a biztonságtudatosság fokozása	7



1 BEVEZETÉS

A szervezet tevékenysége során igénybe vett és a közben keletkező információk, továbbá a normál napi ügyvitelt, és az adatfeldolgozást támogató informatikai és kommunikációs eszközök jelentős információs vagyont képviselhetnek. Bizalmas mivoltuk, megbízhatóságuk, és a hozzáférhetőségük minősége alapvető jelentőséggel bír a Hivatal szolgáltató tevékenysége, jogszabályoknak való megfelelése, illetve jó hírének fenntartása szempontjából.

1.1 Az Informatikai Biztonsági Politika célja

Vácduki Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) Informatikai Biztonsági Politikájának (a továbbiakban: ITBP) célja, hogy a vonatkozó jogszabályoknak megfelelően, figyelembe véve a Hivatal belső szabályozó környezetét, meghatározza azokat a követendő alapelveket, melyek az informatikai és kommunikációs rendszerek által kezelt információs vagyont bizalmassága, sértetlensége, rendelkezésre állásának biztosítása és funkcionalitása, továbbá üzembiztonsága fenntartása érdekében vonatkoznak.

1.1.1 Az információbiztonság keretrendszere

Az információbiztonság keretrendszere, a Hivatal tevékenységének elvárt szintű fenntartásának biztosításával, és annak biztonságos működését veszélyeztető események megelőzésével, továbbá negatív hatásának minimalizálásával foglalkozik.

Ezért cél az, hogy egy olyan kontrolrendszer kerüljön kialakításra, bevezetésre és működtetésre, amely fenntartja a Hivatal folyamatos, elvárt szintű szolgáltató tevékenységét és minimalizálja a működés során felmerült negatív kihatású biztonsági eseményeket.

1.1.2 Az információbiztonság aspektusai

A Hivatal tevékenysége során keletkező információ is vagyonszerűen jelenik meg, és ennek érdekében meg kell tenni azokat a szükséges intézkedéseket, melyek védenek a jogosulatlan elérés, módosítás és megsemmisülés ellen.

Az információ biztonságának három főbb aspektusa van, amelyek a

- **Bizalmasság**, a kezelt információhoz csak az arra felhatalmazott személyek részére legyen elérhető, továbbá az értékes és érzékeny információk megőrzésének biztosítása az illetéktelen hozzáféréstől, illetve annak nyilvánosságra hozatalától;
- **Sértetlenség**, az információ pontosságának, a valóságnak mindenben megfelelő megvédése, beleértve annak jogosulatlan megváltoztatását;
- **Rendelkezésre állás**, az információ szempontjából annak biztosítása, hogy a kezelt rendszerek funkciója, elérhetősége, és az adatok visszakereshetősége megvalósuljon.

A gondosan megfogalmazott informatikai biztonsági alapkövetelmények, a Hivatal számára fontos információk, rendszerek és szolgáltatások rendelkezésre állásának sérülése, az adatokkal való



visszaélések, illetve a Hivatal folyamatos tevékenységében történő fennakadás kockázatainak csökkentésére irányulnak.

1.2 Jóváhagyás

Az informatikai biztonsági politikát - összhangban a Hivatal egyéb céljaival – Vácduka Község Önkormányzatának Képviselőtestülete hagyja jóvá, és hirdeti ki az érintettek számára.

1.3 Az Informatikai Biztonsági Politika felülvizsgálta

Az ITBP-t igény szerint legalább két évente, vagy időközben felmerülő jelentősebb infrastrukturális, továbbá egyéb releváns változás esetén felül kell vizsgálni, és szükség esetén módosítani kell, mind a Hivatali, mind informatikai szakmai szempontok alapján.

1.4 Az Informatikai Biztonsági Politika értékelése

Rendszeresen meghatározott időközönként értékelni szükséges, hogy a politikában meghatározott elvek hogyan valósulnak meg.

1.5 Az Informatikai Biztonsági Politika hatálya

A Hivatal gondoskodik arról, hogy

- az ITBP jogosulatlanok számára ne legyen megismerhető, módosítható, továbbá
- az ITBP-ben foglaltak az érintettek részére ismerté váljon.



1.5.1 Az ITBP alanyi hatálya

Az ITBP alanyi hatálya kiterjed a Hivatal valamennyi teljes vagy részmunkaidős, továbbá szerződéses munkavállalójára.

1.5.2 Az ITBP tárgyi hatálya

Az ITBP tárgyi hatálya kiterjed a Hivatal informatikai rendszerének üzemeltetésében, fejlesztésében és karbantartásában résztvevő cégekre, illetve azon magánszemélyekre, akik közvetve, vagy közvetlenül kapcsolódnak a Hivatalhoz, fizikai elhelyezkedéstől, illetve a tulajdonos, vagy üzemeltető személyétől függetlenül.

1.5.3 Az ITBP időbeli hatálya

Az ITBP időbeli hatálya visszavonásig érvényes.

1.6 Informatikai biztonsági felelős

Az informatikai biztonsági feladatok elvégzésére a Hivatal vezetőjének ki kell jelölni egy Informatikai Biztonsági Felelőst.

1.7 Vezetőségi elkötelezettség

A Hivatal vezetősége számára kiemelt fontossággal bír az informatikai biztonsági keretrendszer működtetése, és elvárja minden érintett személy részéről a politika irányelveinek, és az ehhez kapcsolódó szabályok betartását!

1.8 Kapcsolódó dokumentumok

- Informatikai Biztonsági Stratégia
- Informatikai Biztonsági Szabályzat

2 A KOCKÁZATELEMZÉS ALAPELVEI

A kockázatelemzés során ajánlott figyelembe venni a releváns nemzetközi vagy hazai szabványokat, ajánlásokat, legjobb gyakorlatokat. Informatikai biztonsági szempontból, a kockázatelemzés alapját képezi az adatok és informatikai rendszerelemek bizalmasságának, sértetlenségének és rendelkezésre állásának, és ezek sérüléséből, elvesztéséből bekövetkező káros hatás nagysága, terjedelme, továbbá a káros hatás bekövetkezésének veszélyes mértéke, becsült valószínűsége.

3 AZ OSZTÁLYBA SOROLÁS ALAPELVEI

A biztonsági osztályba sorolás - összhangban a releváns jogszabályokkal -, a kezelt adatok minősége és az informatikai rendszerelemek által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának sérülése esetén potenciálisan bekövetkező káresemény nagyságának és a rendelkezésre álló erőforrások figyelembe vétele alapján történik meg.



Az osztályba sorolás közben, az elvárttól eltérő hiányosságok kiküszöbölésére Intézkedési Tervet kell készíteni.

4 AZ INFORMATIKAI BIZTONSÁG ALAPELVEI

Az informatikai keretrendszer kialakításakor olyan fizikai-, logikai és adminisztratív irányelveket kell megfogalmazni, ami összhangban van a szervezet működésével és a releváns jogszabályokkal.

4.1 A kockázatarányos védelem elve

Az informatikai biztonsági intézkedéseket úgy kell meghatározni, hogy annak költség vonzata arányban álljon a haszon megtérülésével. Az intézkedéseket kockázat arányosan kell mérlegelni, melyeket rendszeresen felül kell vizsgálni. A maradvány kockázatokat a vezetőségnek dokumentáltan el kell fogadnia.

4.2 Teljes körű védelem elve

Az informatikai biztonsági intézkedéseket a Hivatal minden elemére érvényre kell juttatni.

4.3 Az egyenszilárdság elve

Az egyenszilárdság elve szerint, azonos erősségű biztonsági szintek kerüljenek kialakításra minden egyes biztonsági rendszerelem kialakításakor.

4.4 Rendszerfejlesztések biztonsági elv

Az alkalmazások és szolgáltatások fejlesztési életciklusa során a biztonságtudatosság, mint követelmény jelen kell, hogy legyen, a tervezéstől kezdődve egészen a bevezetésig.

4.5 A „négy szem” elv

A Hivatal működése során, annak kritikus folyamataiba felülvizsgálatokat kell beiktatni úgy, hogy a folyamat csak akkor tudjon tovább lépni, ha azt legalább két személy ellenőrizte. Szűrőpróbaszerűen a vezető is gyakorolhat ellenőrzési tevékenységet.

4.6 A szükséges és elégséges hozzáférés elve

A Hivatal rendszereihez és helyiségeihez való hozzáférések szintjét úgy kell meghatározni, hogy az igénybe vevő csak a munkája elvégzéséhez szükséges jogokat kapja meg, és ne többet.

4.7 Fizikai biztonság

A fizikai biztonság kialakításakor cél az illetéktelen hozzáférés megakadályozása. Az informatikai rendszerek külső környezeti hatásoktól való védelmét úgy kell kialakítani, hogy a Hivatal értékei, eszközei, és a szolgáltatás folytonossága ne legyen fenyegetve.

4.8 Vírusvédelem

A rosszindulatú, kártékony alkalmazások ellen naprakész védelmi rendszerrel kell rendelkezni. A felhasználókat oktatásban kell részesíteni, illetve fel kell készíteni őket a megelőző és elkerülő magatartásra.



4.9 Mentés, archiválás

A törvényi kötelezettségeknek megfelelő mentési, archiválási rendszert úgy kell kialakítani, hogy az elvárt feltételek mellett lehetőség legyen az információk visszaállítására. Nem várt esemény bekövetkeztekor, a rendszer, illetve a kezelt adatok visszaállíthatók egy korábbi időpontra, ezzel is csökkentve a kár mértékét.

4.10 Naplózás

Az informatikai rendszer használatát a telepített, illetve beépített lehetőségek (pl. naplózás bekapcsolása) segítségével nyomon kell követni, és gondoskodni kell annak ellenőrzéséről is.

4.11 Incidensek kezelése

A napi normál működés során felmerült informatikai biztonsági fenyegetéseket haladéktalanul jeleneti kell az Informatikai Biztonsági Felelősnek.

4.12 Működésfolytonosság fenntartása

Meg kell határozni azokat a fő irányelveket és módszereket, melyek segítségével fenntartható a kritikus folyamatok, szolgáltatások folytonossága nem várt esemény bekövetkeztekor.

4.13 Oktatás, képzés, - a biztonságtudatosság fokozása

A biztonságtudatosság növelése érdekében oktatásokat, képzéseket kell tartani.

Vácduka, 2016. 11. 17.

Vékás Sándor

Informatikai Biztonsági Felelős



Jónásné Héder Hedvig

Aljegyző