



Qualidat

MAJESTASZÁRTERVÉNY  
Mielőtt döntést hoz...

2015. SZEPTEMBER

Ajánlat

## a Dombrádi Közös Önkormányzati Hivatal

elektronikus információbiztonsági rendszerének  
kifejlesztésére és auditalásra való felkészítésére

Budapest, 2015. augusztus 27.

Vojnisek Péter  
vojnisek.peter@qualidat.hu  
+36 30 201 7554

## Tartalomjegyzék

1. HÁTTÉR INFORMÁCIÓ .....	3
2. JOGSZABÁLYI- ÉS SZABVÁNY-KÖVETELMÉNYEK .....	4
3. A FELKÉSZÍTÉS SORÁN MEGOLDANDÓ FELADATOK .....	5
AZ IT RENDSZER BIZTONSÁGI OSZTÁLYBA SOROLÁSA .....	5
AZ INFORMATIKAI RENDSZER ALAPDOKUMENTUMAI ÉS SZEMÉLYI FELTÉTELEI .....	5
KOCKÁZATELEMZÉS .....	6
AZ IT BIZTONSÁGI RENDSZER ELJÁRÁSAI .....	6
AZ IT BIZTONSÁGI RENDSZER BEVEZETÉSE .....	7
OKTATÁS .....	7
4. AUDIT .....	7
5. KERESKEDELMI AJÁNLAT .....	8



## 1. Háttér információ

A 2013. évi L. törvény és a kapcsolódó rendeletek egzakt követelményeket fogalmaznak meg az önkormányzatok digitális informatikai rendszereinek általános információbiztonsági kialakításával kapcsolatban.

A kérdést eredetileg szabályozó törvények:

- A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (IBTV).
- A 77/2013 (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és szintbe sorolás követelményeiről

Az informatikai rendszerek biztonságainak konkrét követelményeit meghatározó nemzetközi szabványok:

- MSZ EN ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények
- MSZ/T EN ISO 9001:2015. Minőségirányítási rendszerek. Követelmények.

Jelen ajánlatunk a Dombrádi Közös Önkormányzati Hivatal fenti információbiztonsági rendszerének (IBR) kiépítésére és auditra való felkészítésére irányul.

A IBR hatálya lefedi a Hivatal teljes illetékességi területét, nevezetesen az alábbi településekre tejed ki:

- Újdombrád
- Tiszakanyár
- Dombrád

## 2. Jogszabályi- és szabvány-követelmények

A hivatkozott jogszabályok és szabványok döntően az alábbi követelményeket fogalmazzák meg az informatikai rendszerrel kapcsolatban:

- a) Az informatikai rendszernek meg kell felelni az általános információbiztonsági zártági követelményeknek. Az informatikai rendszer akkor felel meg ezeknek a követelményeknek, ha annak tervezése, implementálása és működtetése során az összes releváns veszélyt (fenyegetést) figyelembe vették és a szükséges adminisztratív, logikai és fizikai intézkedéseket megtették.
- b) Az informatikai rendszerhez történő jogosulatlan hozzáférés legyen megakadályozva. Ez akkor teljesül, ha alacsony támadói potenciállal rendelkező támadó összejátszás nélkül, belső információkkal rendelkezve sem képes jogosulatlan hozzáférést szerezni.
- c) A rendszerben tárolt információk észrevétlen módosítása legyen megakadályozva. Ez akkor teljesül, ha az információk módosítása megfelelően védett.
- d) Adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.
- e) Logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.
- f) Fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az előerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

Az információbiztonsági zártág követelményeit a 2013. évi L. törvény (IBTV) határozza meg. Eszerint az IT rendszer zárt, teljes körű, folytonos és kockázatokkal arányos védelmet biztosít a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az IT rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából. Az előbbieken felsorolt védelmi típusok rendszerteknikailag az alábbi tulajdonságokkal rendelkeznek:

- Zárt védelem,
- Teljes körű védelem,
- Folytonos védelem,
- Kockázatokkal arányos védelem.



### 3. A felkészítés során megoldandó feladatok

A felkészítés egymást követő lépései a következők:

#### Az IT rendszer biztonsági osztályba sorolása

Kezdő lépésként elvégezzük a Dombrádi Közös Önkormányzati Hivatal informatikai rendszerének biztonsági osztályba sorolását.

A 2013. évi L. törvény (IBTV) hatálya alá tartozó elektronikus információs rendszert biztonsági osztályba kell sorolni bizalmasság, sértetlenség és rendelkezésre állás szempontjából az IBTV 7§-ában, valamint a 77/2013. (XII. 19.) NFM rendelet 1§ és 1. sz. mellékletben rögzített követelményeknek megfelelően.

Ezt követően meg kell vizsgálni, hogy a Dombrádi Közös Önkormányzati Hivatal informatikai rendszere megfelel-e a biztonsági osztályára vonatkozó követelményeknek. Eltérés esetén intézkedési tervet kell készíteni a megfelelés elérésére.

Az osztályba sorolást az Dombrádi Közös Önkormányzati Hivatal vezetője hagyja jóvá, és jegyezteti be az Informatikai biztonsági szabályzatba.

#### Az informatikai rendszer alapidokumentumai és személyi feltételei

Következő lépésként kidolgozzuk az IT biztonsági rendszer alapidokumentumait, melyek a következők:

- Informatikai biztonságpolitika
- Informatikai biztonsági stratégia
- Informatikai biztonsági szabályzat
- IBR Intézkedési célkitűzések és intézkedések

A fenti dokumentumok kidolgozásánál figyelembe vesszük az MSZ EN ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények c. szabvány követelményeit.

A dokumentumok kidolgozásával egy időben kell kijelölni az információbiztonságért felelős munkatársat. Amennyiben erőforrás hiányában ez nem lehetséges, cégünk vállalja a feladatkör átalánydíjas ellátását. Ennek kapcsán kidolgozzuk a HR feltételekre vonatkozó dokumentumokat, és elvégezzük a szükséges képzést. A HR alapidokumentumok a következők:

- Személybiztonsággal kapcsolatos eljárás (felvételi eljárás, alkalmazási feltételek, munkaviszony megszűnése)
- Képzési eljárásrend (belső biztonsági oktatások, képzések)

## Kockázatelemzés

A kockázat meghatározott veszélyes események valószínűségének és következményei súlyosságának kombinációja. Matematikailag az adott idő alatt a rendszert ért váratlan eseményekből eredő kár várható értéke.

A kockázatelemzés során elvégezzük a veszélyek azonosítását, a kockázatok meghatározását és javaslatot teszünk csökkentésük lehetőségeire és a szükséges intézkedésekre. Az elkészítendő dokumentumok a következők:

- Kockázatkezelési eljárásrend (kockázat menedzsment)
- Az információs adatvagyon felmérése
- IT kockázatelemzés

## Az IT biztonsági rendszer eljárásai

Az általános szabályozók nyomán elkészítjük az IT biztonsági rendszer működését részletesebben szabályozó eljárásokat, melyek a következők:

- Biztonságtervezési eljárásrend
- Rendszerbiztonsági terv
- Az elektronikus információs rendszerek nyilvántartása
- Fizikai védelmi eljárásrend
- Konfigurációkezelési eljárás
- Szoftverek telepítési szabályai
- Üzletmenet folytonosság tervezése
- Mentési eljárás
- Rendszer-karbantartási eljárásrend
- Konfigurációs beállítási eljárás
- Adathordozók védelmi eljárásrendje
- Azonosítás és hitelesítés eljárásrend
- Hozzáférés ellenőrzési eljárásrend
- Azonosítással, hitelesítéssel kapcsolatos eljárásrend
- Távoli hozzáférés szabályozása
- Vezeték nélküli hozzáférés dokumentációja
- Mobil eszközök használata
- Külső hozzáférések szabályozása
- Rendszer- és információsértetlenségi eljárásrend
- Naplózási eljárásrend
- Rendszer- és kommunikációvédelmi eljárásrend
- Biztonsági eseménykezelési eljárás

- Beszerzési eljárásrend
- Külső elektronikus információs rendszerek szolgáltatásainak biztosítása
- Változáskezelési eljárásrend

## Az IT biztonsági rendszer bevezetése

A sikeres audit érdekében a biztonsági rendszert a napi gyakorlatba be kell vezetni, ehhez segítséget nyújtunk. A rendszer azon elemeit pótolni kell, amelyeket a vonatkozó jogszabályok előírnak, és korlátozottan állnak rendelkezésre. A konkrét teendők felmérésére belső auditot tartunk, melynek során a Dombrádi Közös Önkormányzati Hivatal érintett munkatársaival együtt részletesen áttekintjük az IT rendszert.

## Oktatás

A jogszabályok előírják az érintett munkatársak oktatását az IT rendszer biztonságos működtetése és használata érdekében. Annak érdekében, hogy elkerüljük a költséges külső tanfolyamokon való részvételt, ajánlatunk tartalmazza a szükséges tanfolyamok megtartását és a releváns információk és tudás átadását.

## 4. Audit

Az elkészült információ biztonsági rendszert független tanúsító cég végzi. Ajánlatunk sikerdíjas, a projektet a ISO27001:2014-es tanusítvány sikeres megszerzése zárja.

## 5. Kereskedelmi ajánlat

Amennyiben az információbiztonsági rendszer kiépítése 2015. októberben (aláírt szerződéssel) elindul, az auditra való felkészítés a vállalkozó akadályoztatása nélküli esetben biztosítja a **2015. decemberi tanúsítási audit** megtartását.

**A vállalási díj: 950.000 Ft + ÁFA,**

amely összeg tartalmazza a megbízás tárgyát képező, az ajánlatban felsorolt feladatok valamennyi munkadíját és a vállalkozónál felmerült költségét (anyaghasználat, útiköltség, stb.). Nem tartalmazza a Dombrádi Közös Önkormányzati Hivatal IT rendszerének esetleges módosításával és tanúsítvány megszerzésével kapcsolatos költségeket.

Amennyiben az Önkormányzat kezelésében és fenntartási körében jegyzett egyéb intézmények is bevezetik az információ biztonsági rendszert, és a feladatokat egymással párhuzamosan tudjuk végezni, **50%-os kedvezményt adunk** a vállalási és napidíjainkból a csatlakozó intézmények részére!

Ajánlatunk indikatív ajánlat. A felek között történő megállapodás tartalmát és feltételeit közösen pontosítjuk.

Ajánlatunk 30 napig érvényes.





WEB BIZTONSÁG  
INFORMATIKA

## AJÁNLATA

**Csáki Anita és Nagy János Úr részére!**

### **Dombrádi Közös Önkormányzati Hivatal**

**Felkészítő tevékenység** a Hivatal 2013. évi L. törvény (az állami és önkormányzati szervek elektronikus információbiztonsága) szerinti **megfelelésének kialakítására**

**Készítette: Tamás Bence**

**Web Biztonság Informatika Kft.**

*Az informatikai védelem szakértője*

**2015. augusztus 12.**

## **1. Web Biztonság Informatika Kft. ajánlata**

### **Bevezető:**

Cégünk, a Web Biztonság Informatika Kft. küldetése, hogy fejlődjön az informatikabiztonság hazánkban, és segítsük az önkormányzatokat, hogy megfeleljenek az információbiztonsági törvénynek.

Tejesítené a követelményeket, de nincs olyan kollégája, aki legalább 5 év informatikabiztonsági területen szerzett gyakorlattal, vagy a törvényben előírt végzettségekkel rendelkezne? Előzze meg a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) büntetését! Rendelje meg a most kedvezményes ajánlatunkat!

### **Informatikabiztonsági ajánlat**

Az ajánlatunk tartalmazza a 2014. július 1-i határidőig való megfeleléshez szükséges feladatokat. Kollégáik közreműködésével elkészítjük az önkormányzatuk kockázatértékelését és kockázati besorolását a NEIH által módszertanként ajánlott segédlet felhasználásával, valamint létrehozuk a Megrendelő informatikai biztonsági szabályzatát a 2013. évi L. törvény és a 77/2013. (XII.19.) NFM rendelet követelményei szerint.

További részleteket a weboldalunkon olvashat: <http://webteszt.com/biztonsag>

### **Rendszerkövetés – opció**

A törvény előírja, hogy minden önkormányzatnál ki kell nevezni egy személyt informatikabiztonsági felelősnek, aki éves rendszerességgel ellátja az előírt informatikabiztonsági feladatokat.

Amennyiben szeretnék, hogy távmunkában, szakképzett módon ellássuk az informatikabiztonsági felelősi feladatokat, akkor erre külön szerződés keretében tudunk lehetőséget biztosítani.

Rendszerkövetés szolgáltatásban vállalt feladataink:

- Szabályzatok aktualizálása (a jelzett változások alapján)
- Évenkénti egyszeri belső audit (kockázati besorolás a törvény által előírt frissítése)
- Évenkénti egyszeri oktatás (a törvény által előírt évenkénti oktatás megtartása)
- Az informatikabiztonsági rendszer fenntartásához szükséges szakmai tanácsadás, támogatás (telefonon, e-mailben)

## **Ajánlataink:**

### **I. Informatikabiztonsági ajánlat**

Előzetes felmérésünk, és a rendelkezésünkre álló információk alapján az alábbi ajánlatot tesszük. Felkészítő tevékenység a Hivatal 2013. évi L. törvény szerinti megfelelésének kialakításához teljes díja (az ár 30 munkaórát és 1 db kiszállás díját tartalmazza **50%-os kedvezménnyel**):

**Ajánlati ár:** 420.000 Ft + ÁFA

### **II. Rendszerkövetés**

A rendszerkövetés résznél szereplő feladatok alapján az informatikabiztonsági rendszer követésének díja (az ár évi 25 munkaórát és 1 db kiszállás díját tartalmazza 40%-os kedvezménnyel):

**Ajánlati ár:** 35.000 Ft + ÁFA / hó

### **Az ajánlatunk 2015. 08. 31-ig érvényes.**

Az ajánlatban szereplő árak az ÁFA-t nem tartalmazzák!

Az ajánlat egyénre szabott, így az ajánlatot, az ajánlat tartalmát vagy akár az ajánlat tartalmának bármely részét harmadik fél számára kiadni szigorúan TILOS.

Cégünk fenntartja a jogot, hogy a megrendelést (kapacitás hiányában) visszautasítsa, erről a megrendelőt írásban vagy e-mailben értesítjük. Befogadott megrendelésnek az általunk aláírt szerződés minősül.

### **Igényeljen tőlünk szerződéstervezetet!**

Amennyiben ajánlatunk elnyerte a tetszését, jelezze felénk érdeklődését telefonon, vagy e-mailen, és küldjük a szerződéstervezetünket. Informatikabiztonsági szerződéstervezetünk tartalmazza vállalásainkat és a munka pontos menetét. Szerződéstervezetünk igénylése nem jár megrendelési kötelezettséggel!

*"A 2013. évi L. törvénynek való megfeleléshez a Web Biztonság Informatika Kft. szolgáltatását választottuk. Mind szakmailag, mind a hozzáállásuk tekintetében elégedettek voltunk a nálunk végzett munkájukkal. "*

***Moháiné Jakab Anikó jegyző, Vecsési Polgármesteri Hivatal***

### **Miért válassza a Web Biztonság Informatika Kft. informatikabiztonsági szolgáltatását?**

A legjobb ár-érték arányú munka a piacon

Több mint 50 önkormányzati referencia

Az egész ország területén dolgozunk

Referenciánk között a legkisebb néhány fős hivataloktól a legnagyobbakig minden megtalálható

Folyamatos konzultáció a NEIH munkatársaival

Kockázatelemzés és szabályzatkészítés

Tanácsadás

Minőségi és igényes munka

Folyamatos egyeztetés, kapcsolattartás a megbízóval

Szakértői munka egyéb informatikabiztonsági területeken is (etikus hackelés, belső auditok, ISO 27001 bevezetés, stb.)

Jól képzett szakemberek

*"Jót jó áron, egy jó szolgáltatótól."*

***Vincze Jánosné jegyző, Szanki Polgármesteri Hivatal***

További részleteket és véleményeket a weboldalunkon olvashat: <http://webteszt.com/biztonsag>

## 2. Web Biztonság Informatika Kft. bemutatása

<b>A cég elnevezése:</b>	<b>Web Biztonság Informatika Kft.</b>
<b>A cég székhelye:</b>	5600 Békéscsaba, Felsőnyomás 166/1
<b>Adószáma:</b>	24261175-2-04
<b>Telefonszáma:</b>	(+36) 70 236 23 01
<b>E-mail címe:</b>	info@webteszt.com

**Önkormányzati referenciáink** (részletek referenciáink közül):

- o Albertirsai Közös Önkormányzati Hivatal
- o Bucsai Közös Önkormányzati Hivatal
- o Budapesti XXIII. Kerületi Polgármesteri Hivatal
- o Esztergomi Közös Önkormányzati Hivatal
- o Furtai Közös Önkormányzati Hivatal
- o Gödi Polgármesteri Hivatal
- o Kalocsai Közös Önkormányzati Hivatal
- o Keszthelyi Polgármesteri Hivatal
- o Kétújfalui Közös Önkormányzati Hivatal
- o Letenyei Közös Önkormányzati Hivatal
- o Nagyoroszi Közös Önkormányzati Hivatal
- o Ostorosi Közös Önkormányzati Hivatal
- o Szegvári Közös Önkormányzati Hivatal
- o Tamási Közös Önkormányzati Hivatal
- o Tápszentmiklósi Közös Önkormányzati Hivatal
- o Vasaljai Közös Önkormányzati Hivatal
- o Váci Polgármesteri Hivatal
- o Vecsési Polgármesteri Hivatal
- o Záhonyi Közös Önkormányzati Hivatal

Forduljon hozzánk bizalommal!

2015. augusztus 12.

Tisztelettel:

**Tamás Bence Bertalan**

Ügyvezető

**Web Biztonság Informatika Kft.**

(+36) 70 236 23 01



Dániel András  
üzvevezo igazgato  
lipographic Kft.  
1400 Nyiregyhaza, Debreceni út 5  
Adaszani: 10270008 2-15  
MKB  
0305008-270035-0; 10003285