



# **Közbeszerzési rendszerek Informatikai Biztonsági Szabályzata**

1. kiadás

2009.11.19.

## TARTALOMJEGYZÉK

1	Általános rendelkezések .....	3
1.1	A SZABÁLYOZÁS CÉLJA .....	3
1.2	A DOKUMENTUM BESOROLÁSA .....	3
1.3	KAPCSOLAT AZ ELECTOOL INFORMÁCIÓBIZTONSÁGI RENDSZERÉT SZABÁLYOZÓ EGYÉB DOKUMENTUMOKKAL .....	3
1.4	A DOKUMENTUM HATÁLYA .....	4
1.4.1	<i>Személyi hatálya</i> .....	4
2	Az Auction Tool rendszer .....	5
3	E-Tendering rendszer (Sourcingtool) .....	5
4	Információbiztonsági fogalmak és meghatározások .....	6
4.1	ADATBIZTONSÁG .....	6
4.2	BIZTONSÁGI KOCKÁZAT .....	6
4.3	INFORMÁCIÓ .....	6
4.4	AZ INFORMÁCIÓBIZTONSÁG KRITÉRIUMAI .....	6
4.4.1	<i>Bizalmasság</i> .....	6
4.4.2	<i>Sértetlenség</i> .....	6
4.4.3	<i>Rendelkezésre állás</i> .....	6
4.4.4	<i>Elszámoltathatóság</i> .....	6
4.5	BIZTONSÁGI INCIDENS .....	7
4.6	INFORMATIKAI ERŐFORRÁSOK .....	7
4.6.1	<i>Adatok</i> .....	7
4.6.2	<i>Alkalmazások</i> .....	7
4.6.3	<i>Technológia</i> .....	7
4.6.4	<i>Létesítmények</i> .....	7
4.6.5	<i>Munkatársak</i> .....	7
5	Informatikai biztonsági alapelvek .....	8
5.1	ÁLTALÁNOS BIZTONSÁGI ALAPELVEK .....	8
5.2	FIZIKAI VÉDELEM, ÉS A KÖRNYEZET VÉDELME .....	8
5.3	A KOMMUNIKÁCIÓ ÉS AZ ÜZEMELTETÉSI IRÁNYÍTÁSA .....	9
5.4	HOZZÁFÉRÉS-ELLENŐRZÉS .....	9
5.5	INFORMÁCIÓS RENDSZEREK BESZERZÉSE, FEJLESZTÉSE, FENNTARTÁSA .....	10
5.6	INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE .....	10
	<input type="checkbox"/> <i>Információbiztonsági események jelentése</i> .....	10
	<input type="checkbox"/> <i>Biztonsági gyenge pontok jelentése</i> .....	10
	<input type="checkbox"/> <i>Információbiztonsági incidensek és javító fejlesztések kezelése</i> .....	10
	<input type="checkbox"/> <i>Felelőségek és eljárások</i> .....	10
	<input type="checkbox"/> <i>Tanulságok levonása az információbiztonsági incidensekből</i> .....	10
	<input type="checkbox"/> <i>Bizonyítékok gyűjtése</i> .....	10
5.7	A MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA .....	11
5.8	KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS .....	11

## **1 Általános rendelkezések**

### **1.1 A szabályozás célja**

A szabályozás célja a tájékoztatás az Electool Hungary Kft. (Electool) által üzemeltetett közbeszerzésben használatos rendszerek biztonsági- és üzemeltetési-folyamatainak kialakítása során alkalmazott szempontokról az Electool szerződéses partnerei és a szolgáltatást igénybevevők számára. Továbbá azon feltételek és alapelvek felsorolása, amelyek betartása mellett a rendszer folyamatos és biztonságos üzemeltetése fenntartható.

### **1.2 A dokumentum besorolása**

Jelen dokumentum nyilvánosan hozzáférhető, az Electool weboldaláról a hatályos verzió elérhető.

### **1.3 Kapcsolat az Electool információbiztonsági rendszerét szabályozó egyéb dokumentumokkal**

Mivel jelen dokumentum nyilvános besorolású, ezért nem tartalmazhat olyan információt, amely az információbiztonsági rendszer fenntarthatóságát veszélyezteti. A részletes eljárásokat a továbbiakban hivatkozott változó bizalmassági besorolású dokumentumok tartalmazzák.

## **1.4 A dokumentum hatálya**

### **1.4.1 Személyi hatálya**

Jelen szabályzat kiterjed:

- társaságunk valamennyi, a közbeszerzési rendszerekkel kapcsolatos üzemeltetési és fejlesztési feladatokban érintett informatikai feladatot ellátó, adatkezelést, feldolgozást végző munkatársára, valamint
- társaságunk szerződéses partnereire, vagy
- a társaságunkkal más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, vagy titoktartási nyilatkozatok alapján.

## 2 Az Auction Tool rendszer

Az Electool online aukciós szolgáltatása egy integrált, Internet-alapú alkalmazás, mely a gyakorlatban a hozzá kapcsolódó alap és értéknövelt szolgáltatásokra, tanácsadói tevékenységre épül.

Az online aukció sajátossága, hogy a vevő nem a szállítókkal tárgyal, hanem a szállítók egymással versenyeznek annak érdekében, hogy meghatározzák a valós piaci árat és elnyerjék az adott üzletet.

Az online aukcióval támogatott beszerzési folyamat segítségével:

- A vevő valamennyi ajánlattevővel azonos időben tárgyal, ezáltal lehetőség nyílik a transzparens versenyeztetésre
- standardizálni és automatizálni lehet a rutinfolyamatokat
- lerövidül a tárgyaláshoz és szerződéskötéshez szükséges idő
- új szállítók új piacokat szerezhetnek
- mind a vevő, mind a szállító döntéstámogató eszközre tehet szert a célzott és objektív üzleti döntésekhez
- az árajánlat bekérése leegyszerűsödik és lerövidül
- a tranzakciós költségek jelentősen csökkennek (akár 60%-al)
- biztosítható a beszerzési döntések semlegességének és sérthetetlenségének védelme.

## 3 E-Tendering rendszer (Sourcingtool)

Az E-Tendering rendszer egy weben elérhető felület, mely segítségével ajánlatkérési és ajánlatadási folyamatokat lehet elektronikusan leképezni. A rendszer használatának eredményeképp a tenderezési folyamat felgyorsul, az ajánlattal kapcsolatos dokumentáció csak vagy részben csak egészben elektronikusan jön létre.

## **4 Információbiztonsági fogalmak és meghatározások**

### **4.1 Adatbiztonság**

Adatbiztonságon az adatok bizalmosságának, sértetlenségének és rendelkezésre állásának megfelelő színvonalú biztosítását értjük az informatikai rendszerekben.

### **4.2 Biztonsági kockázat**

Az informatikai biztonság sérüléséből és a sérülés valószínűségéből származó kumulált kárérték. A jelentős kárértéket képviselő veszélyforrásokra koncentrált védelmi intézkedésekkel a kockázat elviselhető mértékűre csökkenthető az esetek többségében, azonban figyelemmel kell lenni a törvényszerűen megmaradó és a vezetés által elfogadott maradék kockázatokra.

### **4.3 Információ**

Különböző objektumok összessége, amelyek megjelenési formájukat tekintve igen sokfélék lehetnek: például papíron kinyomtatott szöveg, az informatikai rendszerekben tárolt adatok, műszaki rajzok, hangfelvételek, fényképek, filmfelvételek, egyebek.

### **4.4 Az információbiztonság kritériumai**

#### **4.4.1 Bizalmosság**

Az információt védeni kell a jogosulatlan hozzáféréstől, közzétételtől. Például meg kell akadályozni, hogy a Társaság ügyfeladatai, üzleti titkai nyilvánosságra vagy harmadik fél birtokába kerüljenek, tehát az üzleti információk bizalmossága sérüljön.

#### **4.4.2 Sértetlenség**

Az információ pontosságára, teljességére valamint érvényességére vonatkozik az üzleti értékeknek és várakozásoknak megfelelően.

#### **4.4.3 Rendelkezésre állás**

Az üzleti folyamatokhoz szükséges információ hozzáférhető most és a jövőben. Vonatkozik a szükséges erőforrások és lehetőségeik védelmére is. Például a szerverek meghibásodás nélkül folyamatosan működnek meghatározott ideig.

#### **4.4.4 Elszámoltathatóság**

Minden, az információval, vagy az informatikai rendszerrel kapcsolatos tevékenység egyértelműen azonosítható, utólag visszakövethető kell, hogy legyen.

## **4.5 Biztonsági incidens**

Nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik a működési tevékenységet és fenyegetik az információk biztonságát.

## **4.6 Informatikai erőforrások**

### **4.6.1 Adatok**

Az informatikai rendszerekben keletkezett, tárolt és feldolgozott információk.

### **4.6.2 Alkalmazások**

Az alkalmazások a kézi és programozott eljárások együttese.

### **4.6.3 Technológia**

Az alkalmazott hardverek, operációs rendszerek, adatbázis-kezelő rendszerek, hálózatok, és egyéb informatikai eszközök konkrét megvalósítási formája.

### **4.6.4 Létesítmények**

Az információs rendszert támogató és kiszolgáló egységek halmaza. Például ilyen létesítmény a szerverszoba.

### **4.6.5 Munkatársak**

Az információs rendszereket tervező, beszerző, működtető, kiszolgáló, ellenőrző és felhasználó személyzet.

## 5 Informatikai biztonsági alapelvek

### 5.1 Általános biztonsági alapelvek

Az Electool Hungary Kft. stratégiai céljait és üzleti tevékenységét támogató információs rendszerek, valamint e rendszerek által kezelt, feldolgozott, továbbított adatok bizalmasságát, sértetlenségét, rendelkezésre állását fenyegető veszélyek megelőzésére, felderítésére, elhárítására, enyhítésére vonatkozó általános alapelveket, védelmi feladatokat, intézkedéseket az **Információbiztonsági Politika**, valamint az **Információbiztonsági Szabályzat** tartalmazza.

### 5.2 Fizikai védelem, és a környezet védelme

Az Electool Hungary Kft.-nél a fizikai védelem megvalósítása során a legfontosabb alapelv, hogy azt úgy kell megvalósítani, hogy az megakadályozza a jogosulatlan vagy illetéktelen hozzáférést a társaság információs vagyonához, informatikai eszközeihez

A rendszerek fizikai és a környezeti védelme kiterjed a következőkre:

- Területek védelme, biztosítása
- Berendezések védelme

#### Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 9. fejezet
- Üzemeltetési szabályzat

### **5.3 A kommunikáció és az üzemeltetési irányítása**

Gondoskodni kell az információ-feldolgozó eszközök pontos és biztonságos üzemeltetéséről. Meg kell állapítani valamennyi információ-feldolgozó eszköz üzemeltetésének felelősségeit és szabályait.

Az rendszerekkel kapcsolatban a kommunikáció és az üzemeltetés irányítása a következőkre terjed ki:

- Üzemeltetési eljárások és felelősségi körök
- Harmadik fél szolgáltatásnyújtásának irányítása
- Rendszertervezés és elfogadás
- Védelem a rosszindulatú szoftverek és mobil kódok ellen
- Mentés
- Hálózatbiztonság kezelése
- Adathordozók kezelése
- Információcsere
- Figyelemmel kísérés

#### Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 10. fejezet
- Üzemeltetési szabályzat
- Informatikai rendszerek és eszközök használatának szabályai

### **5.4 Hozzáférés-ellenőrzés**

Az Action Tool hozzáférési jogok kiadására hivatalos eljárásokat kell érvényesíteni.

A Hozzáférés ellenőrzés kiterjed a következőkre:

- A hozzáférés-ellenőrzéshez fűződő működési követelmény
- Felhasználói hozzáférés irányítása
- Felhasználói felelősségek
- Hálózati szintű hozzáférés ellenőrzés
- Operációs rendszer szintű hozzáférés ellenőrzés
- Alkalmazás és információ szintű hozzáférés ellenőrzés
- Mobil számítógép használata és távmunka

#### Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 11. fejezet
- Jogosultság Igénylési Rend
- Üzemeltetési szabályzat
- Informatikai rendszerek és eszközök használatának szabályai

## **5.5 Információs rendszerek beszerzése, fejlesztése, fenntartása**

Az infrastruktúrába, az üzleti alkalmazásokba beszerzése, fejlesztése, fenntartása során a biztonsági követelményeket figyelembe kell venni.

Az Információs rendszerek beszerzése, fejlesztése, fenntartása a következőkre terjed ki:

- Információs rendszerek biztonsági követelményei
- Helyes információfeldolgozás az alkalmazásokban
- Rendszerfájlok biztonsága
- Biztonság a fejlesztési és támogató folyamatokban
- Műszaki sebezhetőség kezelése

### Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 12. fejezet
- ME 7.2 Beszerzés
- Üzemeltetési szabályzat

## **5.6 Információbiztonsági incidensek kezelése**

Az incidenskezelés a következőkre terjed ki:

- Információbiztonsági események és gyengeségek jelentése
  - Információbiztonsági események jelentése
  - Biztonsági gyenge pontok jelentése
  - Információbiztonsági incidensek és javító fejlesztések kezelése
  - Felelősségek és eljárások
  - Tanulságok levonása az információbiztonsági incidensekből
  - Bizonyítékok gyűjtése

### Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 13. fejezet
- Üzemeltetési szabályzat

## **5.7 A Működés folytonosságának irányítása**

A Működés folytonosság irányítás a következőkre terjed ki:

- A működés folytonossága irányításának információbiztonsági szempontjai
- Az információbiztonság belefoglalása a működés- folytonosság irányításának folyamatába
- Működésfolytonosság és kockázatelemzés
- Az információbiztonságot magukban foglaló folytonossági tervek kidolgozása és megvalósítása
- A működés folytonosságának tervezési keretrendszere
- Működésfolytonossági tervek vizsgálata, fenntartása és újraértékelése

Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 14. fejezet
- Üzletmenet folytonossági terv

## **5.8 Követelményeknek való megfelelés**

A Követelményeknek való megfelelés a következőkre terjed ki:

- Jogi követelményeknek való megfelelés
  - Az alkalmazandó jogszabályok megállapítása
  - Szellemi tulajdonjogok
  - Szervezeti feljegyzések védelme
  - Adatvédelem és a személyes adatok titkossága
  - Információ-feldolgozó berendezésekkel való visszaélések megelőzése
  - Biztonsági szabályzatnak és szabványoknak való megfelelés és műszaki megfelelés

Kapcsolódó dokumentumok:

- Információbiztonsági Szabályzat 15. fejezet