2004. évi 4. számú szabályzat a bírósági szervezetek informatikai rendszereinek biztonságos működtetéséről

Az Országos Igazságszolgáltatási Tanács (a továbbiakban OIT) a bíróságok szervezetéről és igazgatásáról szóló 1997. évi LXVI. törvény (a továbbiakban: Bsz.) 39. §-ának k) és q) pontja alapján a bírósági szervezetek informatikai rendszerei biztonságos működtetésének szabályait az alábbiakban határozza meg.

Szabályozás szükségessége

(1) Az informatika helye, szerepe megváltozott, az információ-technológiai eszközökkel támogatott munka egyre hangsúlyosabb szerepet kap a bíróságok életében (hardver, szoftver, hálózat, stb.). Létrejött és működik a bíróságok országos informatikai hálózata, megteremtődtek a feltételei az egész bírósági szervezetre kiterjedő alkalmazási rendszerek bevezetésének. A bírósági szervezetek informatikai stratégiáját az OIT a 2000/68. (XI. 13.) belső határozatával jóváhagyta. Ennek megfelelően a bíróságokon az Országos Igazságszolgáltatási Tanács Hivatala (a továbbiakban OITH) szakmai vezetése mellett nagy értékű, a bírósági folyamatokat nagymértékben érintő informatikai eszközberuházás valósult meg a PHARE, illetve a belső fejlesztési programok keretében.

(2) Az információ-technológia szerepének megnövekedésével megjelentek olyan új tényezők, amelyek mind az informatikai eszközök, mind pedig a rajtuk kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetik. Ezek:

a) Az informatikai rendszerek meghibásodása esetén (hardver-, szoftverhiba, elektromos ellátás hibája stb.) a szervezet működése az elhárítás idejére akár le is állhat.
b) Az Internet, az elektronikus levelezés felhasználásával kártékony kódok (vírusok, férgek stb.) kerülhetnek az informatikai rendszerekbe, amelyek az informatikai rendszerek sérülékenységeit kihasználva jelentékeny rombolást, károkat okozhatnak.
c) Kiszélesedett annak a lehetősége, hogy a bírósági szervezetek az igazságszolgáltatásban közreműködő hatósági szervezetekkel, az ügyfelekkel szélesebb körű, gyorsabb elektronikus információcserét bonyolíthassanak le, amely a folyamatokra, jogosultságokra kiterjedően csak szabályozott keretek között valósítható meg.
d) Megnőtt annak a veszélye is a bíróságok informatikai hálózatában, az együttműködő hálózatok révén, hogy mind a belső, mind a külső felhasználó képes rombolni, titoksértést elkövetni. A hackerek, az anarchista, illetve terrorista csoportok támadásaira egyre hangsúlyozottabban fel kell készülni. Ezek a tevékenységek mind gyakoribbak az informatikai hadviselés területén.

(3) Az informatika területén jelentkező veszélyforrásokkal szemben csak úgy lehet hatékonyan fellépni ha, egy minden területet átfogó (fizikai, személyi, adminisztratív, informatikai biztonsági) szabályozás születik. A bírósági intézmények informatikai infrastruktúrája közös, az ügyviteli-, üzemeltetési folyamatok egymást többszörösen átszövő kapcsolatban állnak, elengedhetetlen az egyenszilárdságú, azonos szervezési

elveken alapuló szabályozás kialakítása. Erre a 2002-ben lefolytatott Állami Számvevőszék vizsgálat is felhívta a figyelmet.

I. fejezet

A szabályzat hatálya

1. §

(1) A szabályzat rendelkezései a Bsz. 16. §-ában felsorolt bírósági szervezetekre (a továbbiakban bíróságok) és az OITH-ra terjednek ki.

(2) A szabályzat rendelkezéseit alkalmazni kell a bíróságok és az OITH informatikai rendszereire, azokra az erőforrásokra, melyek a bíróságok és az OITH ügyviteli folyamataiban az adatfeldolgozást megvalósítják vagy támogatják. Alkalmazni kell továbbá azokra az elektronikus adat és információ feldolgozó tevékenységekre, melyekre az OIT 2002. évi 4. számú, a bíróságok egységes iratkezeléséről szóló szabályzata alapján a titkos ügykezelés szabályain kívül esnek.

(3) A bíróságok és az OITH alkalmazottai szolgálati viszonyuk létesítését követő 30 napon belül kötelesek a bíróságok informatikai biztonsági szabályzatban foglaltakat megismerni, betartásukról nyilatkozni. Azok, akik a szabályzat hatályba lépését megelőzően a bíróságok alkalmazásában álltak 60 napon belül kötelesek írásban nyilatkozni a szabályzatban foglaltak megismeréséről és azok betartásról. A nyilatkozatok a személyi nyilvántartás részét képezik. A bíróságok és az OITH belső szervezeti egységeinek vezetői felelősek a szabályzat rendelkezéseinek megtartásáért.

(4) Az informatikai biztonsággal összefüggő feladatokat a munkaköri leírásokban is rögzíteni kell.

II. fejezet

Értelmező rendelkezések

2. §

1. Adat, adatvagyon, információ:
Az adat a tények, az elképzelések nem értelmezett, de értelmezhető közlési formája.
Adatvagyonnak nevezzük azokat az adatokat, amelyek a bíróságok és az OITH számára értéket képviselnek.
Az információ olyan jelentéssel bíró szimbólumok összessége, amely jelentést hordozó adatokat tartalmaz, és olyan új ismeretet szolgáltat a megismerő számára, hogy ezáltal annak valamilyen bizonytalanságát megszünteti, és célirányos cselekvését kiváltja. Az informatikai biztonság szempontjából információ például (de nem kizárólag): számok és betűk értelmezhető halmaza, szövegek, beszédhangok, rajzok, képek. E vagyontárgyak (adatvagyon) legtöbb esetben nem-tárgyiasult javak.

2. Adatgazda:

Az a szervezeti egység vezető, akinek kötelessége a kezelésébe rendelt adatok titkosságát, sértetlenségét biztosítani, az adatkezelés ügyviteli folyamatát megszervezni, a tevékenység elvégzéséhez szükséges adatoknak a rendelkezésre állásáról gondoskodni az informatikai rendszer működéséhez, és aki jogosult az adatok minősítésére, vagy azok osztályba sorolásának elvégzésére.

3. Adatfeldolgozó rendszer:
Információk meghatározott célú, módszeres gyűjtésére, tárolására, feldolgozására (bevitelére, módosítására, rendszerezésére) továbbítására, fogadására, megjelenítésére, megsemmisítésére stb. alkalmas rendszer. Ez a rendszer számítástechnikai eszközökkel való támogatottsága esetén informatikai rendszernek minősül.

4. Audit:
Az informatikai rendszer meghatározott szabályok szerint megtervezett rendszeres felülvizsgálata, a felülvizsgálati eredmények értékelése és dokumentálása.

5. Bírósági intézmények:
A Legfelsőbb Bíróság, ítélőtáblák, megyei (fővárosi) bíróságok, Országos Igazságszolgáltatási Tanács Hivatala.

6. Bírósági intézmények vezetői:
Legfelsőbb Bíróság elnöke, ítélőtáblák elnökei, megyei (fővárosi) bíróságok elnökei, Országos Igazságszolgáltatási Tanács Hivatalának vezetője.

7. Bírósági szervezetek vezetői (a szabályzat alkalmazása szempontjából):
Legfelsőbb Bíróság elnöke, elnökhelyettesei, főtitkára, kollégiumvezetői, ítélőtáblák elnökei, elnökhelyettesei, kollégiumvezetői, megyei (fővárosi) bíróságok elnökei, elnökhelyettesei, kollégiumvezetői, helyi (munkaügyi) bíróságok elnökei, bírósági intézmények gazdasági hivatalainak, valamint az informatikai szervezeteinek vezetői és helyetteseik, az OIT Hivatalának vezetője és helyettese(i), főosztályvezetői és helyettesei, osztályvezetői.

8. Biztonsági környezet:
A biztonsági környezet a jogszabályok, a szervezet belső szabályai, és elvárásai, szokások, szakértelem és tudás, amelyek meghatározzák azt a környezetet, amelyben az erőforrásokat a szervezet használni akarja.

9. Biztonsági követelmény:
Az informatikai biztonság az informatikai rendszer olyan kielégítő mértékű állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos..

10. Biztonsági tudatosság:
A veszélyforrások felismerése, a védelmi intézkedések szükségességének elfogadása, és rendeltetésszerű végrehajtására való törekvés.

11. Egyenszilárdság:
Az informatikai rendszer minden pontján a védelem azonos ellenállóképességgel rendelkezik.

12. Ellenőrzött forrás:
Ellenőrzött forrásnak tekintett minden, a bíróság szervezetén belül keletkezett, továbbított és köröztetett adat keletkezési helye, ha a készítő egyértelműen meghatározható, azonosítható. Ellenőrzött forrású adathordozó az ilyen adatokat tartalmazó adathordozó.

13. Feladatelhatárolás:
Az informatikai rendszer használatához és üzemeltetéséhez kapcsolódó biztonságkritikus munkakörök szétválasztása.

14. Felelősségre vonhatóság:
Olyan tulajdonság, amely lehetővé teszi, hogy egy adott folyamat tevékenységei egyértelműen az adott folyamatra legyenek visszavezethetők.

15. Határvédelmi rendszer
A bírósági országos informatikai hálózat (belső) és más egyéb külső hálózatok (Internet, Belügyminisztérium-, Legfőbb Ügyészségi-, Büntetés Végrehajtási Országos Parancsnokság hálózatai stb.) között kialakított biztonsági rendszer, amely a belső hálózat rendszereit és adatait védi a külső irányított és esetleges támadásoktól. Alapegységei a tűzfal, a behatolás detektáló, a külső belépő autentikációja és a naplózása.

16. Hitelesség:
Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

17. Hozzáférés:
Olyan eljárás, amely valamely informatikai rendszer arra jogosult használója számára elérhetővé tesz a rendszerben tárolt adatokat. A hozzáférést a legtöbb esetben megelőzi a hozzáférni szándékozó azonosítása.

18. Informatikai alkalmazás:
Az informatikai rendszer egyik eleme, egy előre részletesen meghatározott feladatkör ellátására szolgáló szoftver, mely kihasználja az informatikai eszközök funkcióit.

19. Informatikai Biztonsági Szabályzat (IBSZ):
Olyan belső intézkedés, amely a bírósági intézményeken belül, illetve a köztük lévő infrastruktúrán működtetett informatikai rendszerekre vonatkozóan szabályozza az informatikai rendszerrel kapcsolatos biztonsági intézkedéseket, szervesen illeszkedve a szervezet egyéb működési és ügyrendi előírásaihoz.

20. Informatikai erőforrás:

Informatikai erőforrások az informatikai rendszer, valamint az üzemeltető és az informatikai rendszer szolgáltatásait használó humán erőforrások, alkalmazások, valamint az adatok.
Az adatok, alkalmazások, technológiák (hardver és szoftver), kisegítő eszközök (klíma, energia ellátás stb.), emberek összessége.

21. Informatikai eszköz:
A bíróság által üzemeltetett felhasználói munkaállomás, kiszolgáló, alkalmazás szerver és alkalmazás, hordozható számítástechnikai vagy telekommunikációs eszköz (amennyiben adatátviteli szempontból csatlakozik a bíróság országos informatikai hálózatához), Internet/Intranet kiszolgáló, adathálózati eszköz (hardverek) a működést biztosító szoftverekkel egyetemben, melyek a bíróság munkafolyamatainak támogatására szolgálnak.

22. Informatikai rendszer:
A bírósági intézmények, szervezetek által üzemeltetett, adatok összegyűjtésére, tárolására, feldolgozására, és továbbítására szolgáló rendszer, informatikai eszközök halmaza. Ide tartoznak a technológiák és hardverek – beleértve a felhasználói munkaállomásokat, a kiszolgálókat, alkalmazásszervereket, hordozható számítástechnikai eszközöket, Internet/Intranet kiszolgálókat és adatkapcsolatokat, hálózati és kommunikációs eszközöket, a környezeti infrastruktúrát, valamint az alkalmazásokat.

23. Informatikai szervezet:
A bírósági intézmények informatikai főosztályai, osztályai, csoportjai.

24. Informatikai vezető:
A bírósági intézmények informatikai főosztályainak, osztályainak, csoportjainak vezetője.

25. Informatikus:
Az informatikai feladatokat főállásban ellátó alkalmazott.

26. Jogosultság:
A lehetőség megadása tevékenység végrehajtására. Az információs rendszerek kezeléséhez, azok adatainak eléréséhez különböző szintű jogosultságok tartozhatnak. Vannak informatikai rendszerek és adatok, melyeknek kezelése nincs autentikációhoz kötve, mindenki szabadon használhatja. Vannak olyan információk melyeknek elérése és felhasználása korlátozott, csak egyedileg azonosítható jelszavakkal kezelhetőek. A hozzáférések engedélyezése több szintű, van amit az adott informatikai rendszer adatgazdája engedélyez, van amit egy adott szervezet vezetője és van amit külső intézmény szigorú autentikációval engedélyez, pl. Belügyminisztérium, ügyészség, stb.

27. Kártékony kód:
Olyan program vagy program részlet, mely nem tartozik rendeltetésszerűen az informatikai rendszerhez és a felhasználó vagy informatika engedélye nélkül jogosulatlan tevékenységet végez.

28. Kockázat:

Annak veszélye, hogy egy esemény, fenyegetettség bekövetkezése vagy intézkedés hátrányosan befolyásolja egy szervezet lehetőségeit céljainak és stratégiájának megvalósítása során. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze.

29. Környezeti infrastruktúra:
Az informatikai rendszeren kívül eső, de annak működéséhez feltétlenül szükséges berendezések, elemek halmaza, mely biztosítja a hardverek és technológiák működését, mint pl.: klimatizálás, áramellátás, fizikai hozzáférés védelem stb.

30. Rendelkezésre állás:
A rendszer olyan állapota, amelyben eredeti rendeltetésének megfelelő szolgáltatásokat tud nyújtani (funkcionalitás) meghatározott helyen és időben (elérhetőség).

31. Rendszergazda:
Az informatikán belül egyes informatikai rendszerrel kapcsolatban kiemelt jogosultsággal rendelkező informatikus.

32. Sértetlenség:
Az adat létének, hitelességének, épségének, önmagában teljességének kritériuma, avagy az információ és feldolgozásmódja pontosságának és teljességének a megóvása.

33. Titkosság (bizalmasság):
Az adatnak az a jellemzője, hogy csak egy előre meghatározott felhasználói kör (jogosultak) részére hozzáférhető, mindenki más számára nem. A titkosság elvesztése a felfedés, mely esetén a bizalmas információ az arra jogosulatlanok számára is ismertté, hozzáférhetővé válik.

III. fejezet

Az informatikai biztonság irányelvei

3. §

(1) Infrastruktúrához kapcsolódó védelmi intézkedések:

a) A bírósági szervezeti egységek országos kiterjedésű informatikai hálózaton csatlakoznak egymáshoz. A bírósági intézmények egységein kívül eső szervezetek hálózataihoz kapcsolódni egy ponton, az OIT Hivatala által üzemeltetett határvédelmi rendszerén keresztül lehet. A szűk sávszélesség miatt az ettől eltérő külső csatlakozásra engedélyt az OIT Hivatalának vezetője adhat ki az érdekeltek bevonásával.
b) A bírósági informatikai hálózatán kívül eső szervezetek rendszereinek használatát, biztonsági szabályait külön megállapodások rögzítik.
c) Központilag, - az OIT Hivatala által – országos szinten fejlesztett és működtetett rendszerek informatikai biztonsági szabályozásról az OIT Hivatala gondoskodik.
d) A bírósági intézmények egységes informatikai infrastruktúrájához csak a bírósági intézmények tulajdonában lévő, illetve azok a más tulajdonú informatikai

eszközök csatlakoztathatók, melyek kapcsolódását a bírósági intézmények vezetőinek véleményét kikérve az OIT Hivatalának vezetője engedélyezte.

e) A bírósági intézmények informatikai eszközein csak az informatika által telepített vagy ellenőrzött, jogtiszta, gyári vagy az eszközgazdálkodási szabályzatban foglaltak szerint bevizsgált egyedi fejlesztésű, dokumentált szoftvereket szabad használni.
f) A bírósági intézmények minden számítógépes munkaállomására és minden, a vírusvédelmi rendszer által támogatott kiszolgálójára vírusvédelmi rendszer telepítése és használata kötelező.
g) A bírósági intézmények országos informatikai hálózatát vírusvédelmi rendszerrel kell ellátni.
h) Az informatikai eszközök konfigurációs beállításainak változtatását csak és kizárólag az informatikai eszköz felelős üzemeltetője végezheti.
i) A szerverek, hálózati eszközök elhelyezését úgy kell kialakítani, hogy illetéktelen személy fizikailag ne férhessen hozzájuk, elemi károktól védettek legyenek, illetve a gyártó által meghatározott üzemeltetési feltételek (hőmérséklet, por és páratartalom előírt mértéke) teljesüljenek. Védelmük megfeleljen a rajtuk tárolt és feldolgozott adatok biztonsági besorolása által megkövetelt szintnek.

(2) Adatokhoz kapcsolódó védelmi intézkedések:

a) A titkos ügykezelés szabályai alá tartozó adatokat, információkat a bírósági intézmények informatikai hálózatán továbbítani tilos!
b) Az adatokhoz a jogosult hozzáférésének biztosítása érdekében az informatikai rendszereket minden esetben egyedi, a felhasználó azonosítását lehetővé tevő jelszóval és felhasználónévvel kell védeni, továbbá a jelszavakat bizalmasan kell kezelni, és megfelelő bonyolultságúnak kell lenniük.
c) Az elektronikusan tárolt adatokat a mellékelt minta IBSZ-ben rögzített módszer szerint minősíteni kell. Az adatok minősítése, a hozzáférésre jogosultak körének és a hozzáférés módjának meghatározása az adatgazda felelőssége. A bírósági intézmények dolgozóinak autentikációs jogait az illető személyi anyagában kell megőrizni.
d) A kártékony kódok ellen több szintű védelmet kell kialakítani, úgymint: központilag felügyelt vírusvédelmi rendszert, tartalomszűrő szolgáltatást, valamint növelni kell a munkatársak biztonságtudatosságát.
e) Az informatikus kötelessége a szervereken tárolt szoftverek és adatok (rendszerenkénti és szerverenkénti) mentése. A munkaállomáson tárolt adatok mentése a felhasználó felelőssége.
f) A bírósági intézmények alkalmazottai részére az informatikának biztosítani kell munkavégzésükhöz szükséges informatikai eszközöket, egyértelműen és visszakereshetően kezelnie kell az alkalmazottak belépésével és kilépésével kapcsolatos informatikai feladatokat (eszköz átadás/átvétel), valamint az autentikációs nyilvántartást.
g) A felhasználókat informatikai biztonsági oktatásban kell részesíteni a biztonsági tudatosság elsajátítása érdekében, hogy megértsék és elsajátítsák a jelen, továbbá az Informatikai Biztonsági szabályzatban foglaltakat, felhasználói előírásokat, megismerjék azokat az adatok épségét kockáztató veszélyforrásokat, amelyek számítástechnikai eszközök felhasználása során jelentkezhetnek.

h) Az Internet szolgáltatásait – böngészést, elektronikus levelezést – a munkavégzés céljából lehet igénybe venni. Tilos olyan adat továbbítása (küldése, letöltése), amely alkalmas kártékony kódoknak a bíróságok informatikai rendszerébe juttatására, valamint tilos minden olyan tevékenység, amely jogsértő. Nem szabad a szolgáltatásokat semmilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt sértő módon használni. (Erre vonatkozó nyilatkozatot az elnöki iratok között kell megőrizni.)
i) Elektronikus levélben csak nyilvános információ továbbítható harmadik félnek, kivéve akkor, ha a harmadik féllel az elektronikus levelezés erős titkosítása megoldott és a titkosító kulcscsere megtörtént.
j) A bíróságok országos informatikai hálózat (WAN) kapcsolatainak felügyeletét a külső kapcsolati ponttól a bíróságok adatbemeneti hálózati eszközéig (routerek) az OIT Hivatal informatikája, míg a bírósági belső hálózati (LAN) felügyeletét az adott bírósági intézmény informatikája biztosítja.
k) Az OIT Hivatala mint a bírósági országos informatikai hálózat üzemeltetője rendszertámogatást nyújt a hálózat informatikai elemeire. Az informatikai rendszerben tárolt adatok védelmében biztosítani kell, hogy sem az OITH-ban kialakított országos rendszerfelügyelet és „helpdeszk", sem a bíróságok helyi rendszerfelügyeletét ellátó személyek más szervezeti egység adatait jogosulatlanul ne érjék el.
l) Ha a rendszertámogatás miatt erre mégis szükség van, akkor előzetes egyeztetés és engedélyezés után lehet csak a gépeken a konfigurálást, javítást elvégezni, illetve a távoli gép képernyőjét átvenni és azon munkát végezni.
m) A felhasználó gépéhez az informatika távoli elérés útján is hozzáférhet. A képernyő távoli eléréssel történő átvétele csak a felhasználó előzetes tájékoztatása után történhet.

(3) Szoftverekhez kapcsolódó védelmi intézkedések:

a) Az informatikai biztonság egyenszilárdságának fenntartása érdekében tervszerűen és szabályozottan kell végezni az informatikai rendszerek fejlesztését, ellenőrzését és karbantartását.
b) A bírósági intézmények országos informatikai hálózatán csak olyan szoftver működtethető, amelyek megfelelnek a 2003. évi 3. számú informatikai eszközgazdálkodási szabályzat szoftverbevizsgálási szempontjainak. Ennek megfelelően a bíróságok informatikai hálózatában lehetőleg
   - csak bevizsgált,
   - nyílt (gyártó független),
   - integrálható,
   - kompatibilis és naprakészen dokumentált szoftverek telepíthetők és működtethetők.

(4) Személyekhez kapcsolódó védelmi intézkedések:

a) Feladatelhatárolás elvének betartása.
b) Belépés, kilépés, áthelyezés, helyettesítés informatikai nyomon követhetősége (együttműködés a személyzeti változásokért felelős szervezeti egységgel és annak vezetőjével).

c) Oktatás, számonkérés.
d) Felhasználói fegyelem kialakítása (evés, ivás, dohányzás munkaállomás közelében).
e) Biztonsági tudatosság kialakítása, fejlesztése.

IV. fejezet

Az informatikai biztonság megvalósításában felelős szervezetek és személyek

4. §

(1) Az **OIT** szabályzatban határozza meg a teljes bírósági informatikai rendszer biztonsági eljárásait és követelményeit.

(2) Az OIT hatáskörében eljáró OIT **Hivatala** szakmai iránymutatásával és felügyeletével, módszertani anyagok és ajánlások kiadásával biztosítja a bírósági informatikai hálózat egyen szilárd működését.

(3) A **bírósági intézmény vezetője** kiadmányozza elnöki, illetve hivatali rendelettel az IBSZ-t, biztosítja annak megismerését és oktatását az alkalmazottak részére, intézkedik az IBSZ előírásait megszegő alkalmazottal szembeni eljárás megindításáról.

(4) A **bírósági szervezetek vezetője** a hozzá beosztott alkalmazottakkal betartatja az informatikai biztonsági szabályzatban foglalt követelményeket.

(5) Az **informatikai vezető** előkészíti a jelen szabályzat alapján kötelezően elkészítendő bírósági, hivatali IBSZ-t, valamint az IBSZ alapján a bíróságra, hivatalra egyedileg meghatározott Informatikai Eljárásrendeket.

(6) Az **informatikai biztonsági ellenő**r az informatikai biztonság követelményeinek teljesülését felügyeli, ellenőrzi, szükség esetén eljár a biztonsági szabályokat megszegővel szemben.

(7) **Adatgazda** kötelessége a kezelésébe rendelt adatokkal kapcsolatos információ biztonsági feladatokat ellátni.

(8) **Felhasználó** (bírósági intézményi dolgozó) kötelessége a számára biztosított informatikai eszközt használni (hardver, szoftver), a szabályzatban meghatározott módon használni, alkalmazni.

5. §

(1) Az informatikai biztonsági ellenőr joga és kötelessége:
a) megállapítani, hogy a hatályos törvényi előírásokat a bírósági szervezetek megtartják-e, a kialakított informatikai rendszerek védelme megfelel-e az OIT

által kiadott iránymutatásoknak, belső szabályzatoknak, valamint az érvényes hazai és nemzetközi ajánlásoknak;

b) jelenteni minden informatikai biztonsággal kapcsolatos eseményt közvetlenül a bírósági intézmény vezetőjének, illetve az OIT Hivatal vezetőjének, és véleményét, álláspontját kérni;

c) beruházások során értékelni és ellenőrizni a bíróságok vagy az OIT Hivatala által irányított informatikai a fejlesztést az informatikai biztonság szempontjából, meghatározni a kockázatokat, és javaslatot tenni a szükséges óvintézkedések bevezetésére;

d) a bíróságok vagy az OIT Hivatal által vezetett informatikai beruházások során az informatikai eszközök és a szolgáltatás beszállítók biztonsági szempontból történő minősítése, szükség esetén vizsgálat lefolytatása;

e) éves ellenőrzési terv készítése, mely kiterjed az informatikai erőforrások hasznosítására. Az éves ellenőrzési terv egyeztetése és jóváhagyatása a bírósági intézmények vezetőjével;

f) az éves ellenőrzési tervnek megfelelően az ellenőrzések lefolytatása, és éves jelentés keretében a megállapítások előterjesztése a bírósági intézmény vezetőjének és a hivatali informatikai biztonsági ellenőrnek;

g) a bírósági intézmény vezetőjének utasítására (a hivatali biztonsági ellenőr javaslata alapján) eseti, célirányos ellenőrzések végrehajtása;

h) minden biztonsági esemény kezelése, dokumentálása, felderítése, szankcionálásra javaslat tétel;

i) az IBSZ oktatásának számonkérésének megszervezése.

A hivatali informatikai biztonsági ellenőr további feladatai:

j) az OITH szakmai iránymutatásainak érvényre juttatása az informatikai biztonság területén a bírósági intézmények és az OITH informatikai rendszerében, ezáltal lehetővé téve az egyenszilárdságú, a mind magasabb színvonalú szolgáltatási szint elérését;

k) éves ellenőrzési terv készítése, mely kiterjed a bírósági intézmények, valamint a területükön működő bíróságok és az OITH informatikai erőforrásainak biztonságos működtetésére. Az éves ellenőrzési tervet az OIT hagyja jóvá;

l) az éves ellenőrzési tervnek megfelelően az adott bírósági intézmény vezetőjének előzetes tájékoztatása után az ellenőrzések lefolytatása a bírósági intézmények és az OITH informatikai rendszerein, és a megállapításoknak éves jelentésben az OIT elé terjesztése;

m) a bírósági ellenőrök éves ellenőrzési terveinek jóváhagyása, munkájuknak iránymutatásokkal segítése, valamint felügyelete;

n) az OIT utasítására eseti, célirányos ellenőrzések végrehajtása.

(2) Az informatikának azokon a szakterületein, amelyeken a saját ellenőrzés nem, vagy nem kielégítő hatékonysággal hajtható végre, a informatikai biztonsági ellenőr feladata, hogy az intézmény vezetőjének megkeresésével az OIT Hivatalának vezetőjénél kezdeményezze az informatikai biztonságra szakosodott külső céggel az átvilágítást, a vizsgálat elvégzését (a közbeszerzésre vonatkozó jogszabályok keretei között).

V. fejezet

Az Informatikai Biztonsági Szabályzat

6. §

(1) Az IBSZ a bíróságok és az OIT Hivatalának belső szabályzati rendszerének szerves része. Kapcsolódik a Szervezeti és Működési Szabályzathoz, az OIT 2002. évi 4. számú, a bíróságok egységes iratkezeléséről szóló szabályzatához, és az OIT Hivatala esetében az OIT Hivatalának Iratkezelési és Irattározási Szabályzatához.

(2) E szabályzat melléklete a bíróságok Informatikai Biztonsági Szabályzatának mintája, az adott viszonyokra alkalmazásával – a helyi sajátosságoknak megfelelően – a bírósági intézmények készítik el belső szabályzatukat.

(3) Az IBSZ – az informatikai biztonsággal kapcsolatban a feladatköröket, felelősségi – és hatásköröket, valamint az informatikai erőforrások biztonságos működéséhez szükséges feltételeket határozza meg. Az IBSZ-ben kell rögzíteni azokat az egységes keretszabályokat, értelmezéseket, iránymutatásokat is, amelyeket az informatikai eszközök üzemeltetőinek, fejlesztőinek, felhasználóinak és az adatgazdáknak be kell tartaniuk.

(4) Az IBSZ módosítását kezdeményezhetik a bírósági vagy a hivatali ellenőrök, illetve a bíróságok vagy az OITH informatikai vezetője.

(5) A bíróságok IBSZ-ének meglétét, pontosságát a hivatali informatikai biztonsági ellenőr ellenőrzi.

Az Informatikai Biztonsági Szabályzat felépítése

7. §

Az IBSZ a következő fő részekre tagolódik:

1) **I fejezet: Általános Informatikai Biztonsági Előírások**
Ez egy korlátozott hozzáférésű dokumentum, amely az egyes bírósági szervezetek informatikusainak, a bírósági és hivatali ellenőrnek, valamint az adatgazdáknak a jogait és kötelességeit határozza meg. Célja - a technológiai megoldások részletezése nélkül - általánosan meghatározni az informatikai erőforrások biztonságos működéséhez szükséges feltételeket, a feladat- és felelősségi köröket.

2) II. fejezet: Az Informatikai Felhasználói Előírások
Az általános Informatikai Biztonsági Előírások rendelkezéseiből levezetve rögzíti a felhasználók kötelességeit, az általuk elvégezhető és tiltott tevékenységeket, a számonkérés formáját, valamint a biztonsági események jelentésével kapcsolatos kötelezettségeket. Az Informatikai Felhasználói Előírások fejezet alapja a felhasználói oktatásoknak, melyeken az alkalmazottaknak kötelességük részt venni, és nyilatkozni, hogy a szabályzat tartalmát megismerték, magukra nézve kötelezőnek tekintik. Ha nem vett részt az oktatáson, vagy nem írta alá az oktatási naplót, akkor az informatikai rendszereken, azok támogatásával tevékenységet nem végezhet.

3) **III. fejezet: Informatikai Eljárásrend**
A bíróságok egyes informatikai rendszereire részletesen lebontott, az Általános Informatikai Biztonsági Szabályok helyi speciális rendelkezéseit, a technikai feladatokat részletesen meghatározó szabályokat tartalmazza. Az informatikai vezető készíti el, és az informatikai biztonsági ellenőr jóváhagyásával adja ki. Ez a technikai lehetőségektől függően folyamatosan változhat.
Az Eljárásrendnek legalább az alábbi munkautasításokat kell tartalmaznia:

A bíróság informatikai szervezetének munkarendje
Hozzáférési jogosultságok kezelése
Mentési és archiválási rend
A vírusvédelmi rendszer üzemeltetése
A bíróság informatikai eszközekeinek telepítése

(Az Eljárásrend folyamatosan bővülhet, ehhez az OIT Hivatalának Informatikai Főosztálya folyamatosan ad ki ajánlásokat, módszertani útmutatókat a technikai feltételek változásának függvényében.)

VI. fejezet

Az adatvagyon érzékenységének meghatározása

8. §

Az információrendszerek természetüknél fogva különböző érzékenységű, bizalmasságú információkat kezelnek. Ezeket az adatokat jellemzőjük alapján különböző kategóriákba kell besorolni, amely kategória meghatározza, hogy milyen eljárást kell alkalmazni az adott szinten.

1) A bírósági szervezetek esetében az adatgazda kötelessége a kezelésébe rendelt és informatikai eszközökön feldolgozott adatok érzékenységnek meghatározása, az adatvagyon leltár elkészítése a mellékelt minta IBSZ alapján.

2) Az adatgazda joga és kötelessége
   a) a besorolást eljuttatni a bíróság, illetve a hivatal informatikai biztonsági ellenőréhez;
   b) az általa kezelt adatvagyonban bekövetkezett változás esetén a szükséges értékeléseket ismételten végrehajtani;
   c) szükség esetén a besorolás módosítását kezdeményezni;
   d) az általa elkészített besorolást legalább kétévenként felülvizsgálni.

VII. fejezet

Az informatikai erőforrások biztonsági besorolása

9. §

Az informatikai vezető kötelessége, az informatikai rendszereket egyrészt az informatikai rendszer által feldolgozott adatok érzékenysége alapján, másrészt az adott technikai

eszköznek a hálózatban betöltött szerepe alapján, a mellékelt minta IBSZ-ben rögzített biztonsági szintbe besorolni, és meghatározni környezeti és kezelési feltételeit..

VIII. fejezet

Záró rendelkezések

10. §

A bíróságoknak és az OITH-nak a jelen szabályzatban foglaltak, valamint a mellékelt minta IBSZ alapján, el kell készíteniük a saját IBSZ-üket. A hivatali informatikai biztonsági ellenőr az elkészült IBSZ-eket megvizsgálja, és a tapasztalatokról tájékoztatja az Országos Igazságszolgáltatási Tanácsot.
A szabályzat mellékletét képező minta IBSZ szövegén, az időközben megváltozott informatikai biztonsági feltételekben bekövetkezett módosításokat a OITH szükség szerint folyamatosan, illetve minden év március 1-ig átvezeti, melyet a bíróságok és az OITH a saját IBSZ-ükön szintén szükség szerint folyamatosan, illetve minden év május 1-ig kell átvezetniük.
A szabályzat 2005. január 1. napján lép hatályba.