TANÚSÍTVÁNY
KARBANTARTÁSI
Jegyzőkönyv

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft, mint a Nemzeti Akkreditációs Testület által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet
Tanúsítvány karbantartás eljárás keretében tanúsítja,
hogy a

Közigazgatási és Igazságügyi Minisztérium
E-Közigazgatásért Felelős Helyettes Államtitkárság által fejlesztetett

„Hivatalos Lapkiadás Rendszer”

2013. június 03-i /v1.0/ rendszerverziója

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

a KIB 28-as Ajánlásban szereplő MIBÉTS módszertan alapján
fokozott garanciaszinten értékelve, tanúsítva

alkalmas

a Rendszerbiztonsági előirányzatban meghatározott
azonosítás és hitelesítés, folyamatos működés, hozzáférés ellenőrzés, naplózás és elszámoltathatóság, rendszer- és információ sértetlenség, rendszer és kommunikáció védelem műszaki biztonsági követelményeinek az érvényesítésére.

Jelen tanúsítvány a HUNG-TJ-MIBÉTS-06-2013 számú Tanúsítási jelentés alapján került kiadásra.

Készült a Közigazgatási és Igazságügyi Minisztérium E-Közigazgatásért Felelős Helyettes Államtitkárság megbízásából.

A tanúsítvány regisztrációs száma: HUNG-TK-MIBÉTS-06/1-2013.

A tanúsítás kelte: 2013. június 10.

A tanúsítvány érvényességi ideje /évenkénti felülvizsgálat mellett/: 2016. március 31.
Összesen mellékletekkel 5 oldalon.

PH.

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

Azonosító adatok és a tanúsított rendszer főbb funkciói

Azonosító adatok

A rendszer elnevezése:	Hivatalos Lapkiadás Rendszer
A technológiai értékelés alapja:	2013. 06. 03-i állapot
Rendszer fejlesztő:	Közigazgatási és Igazságügyi Minisztérium
Rendszer működtető:	Közigazgatási és Igazságügyi Minisztérium
Rendszer üzemeltetők:	Publikációs alrendszer: KEKKH (Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala), Külső és belső WMS alrendszer: MHK (Magyar Közlöny Lap- és Könyvkiadó) A telephelyek közötti NTG hálózat: NISZ Zrt.
Tanúsító:	Hunguard Kft.

A tanúsított rendszer főbb funkciói

A Hivatalos Lapkiadás Rendszer a Magyar Közlöny és a Hivatalos Értesítő (továbbiakban: hivatalos lapok) elektronikus megjelentetésének teljes munkafolyamatát támogató informatikai rendszer. A három alrendszer által támogatott teljes munkafolyamat kiterjed az alábbiakra:

- a hivatalos lapok kiadásának szerkesztési folyamatának zárt rendszerben történő elhelyezése (belső WMS alrendszer),
- a hivatalos lapok kiadásához szükséges külső kapcsolatok (külső feltöltés) lehetőségének biztosítása (külső WMS alrendszer),
- a hivatalos lapok egységes és zavartalan megjelenését támogató publikálási felület, (publikációs alrendszer),
- a rendszer adatainak mentése (a publikációs alrendszer tartalmazza az adatmentő szervert is).

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a Hivatalos lapkiadás rendszer biztonságához.

Az értékelés – a Rendszer biztonsági előirányzatban meghatározott – üzemeltetési környezetre vonatkozó biztonsági feltételrendszer teljesülése esetén ad garanciákat a rendszer biztonsági tulajdonságainak érvényesülésére.

A. Risk_Assessment[1]

A rendszer működtetője rendszeres időnként felméri a szervezeti működés során jelen lévő, a rendszer működéséből és kapcsolódó információ feldolgozó, tároló vagy átviteli műveletekből származó biztonsági kockázatokat és a rendszer értékeit.

A.Security_Assessments

A rendszer működtetője:

a) rendszeres időközönként értékeli az IT rendszer biztonsági intézkedéseit, annak megállapításához, hogy az intézkedéseket hatékonyan alkalmazzák-e;
b) intézkedési tervet készít és hajt végre a hiányosságok korrigálására, a rendszerekben meglévő sebezhetőségek csökkentésére vagy kiküszöbölésére;
c) engedélyezteti (akkreditáltatja) az informatikai rendszer működését és bármilyen rendszerkapcsolatot, kapcsolódást;
d) folyamatosan felügyeli, ellenőrizi a biztonsági intézkedések betartását a hatékonyság folytonosságának biztosítása érdekében.

A.Physical_Protection

A rendszer működtetője és üzemeltetője

a) a jogosult felhasználókra korlátozza a rendszerhez, berendezéseihez és kapcsolódó üzemeltetési környezetéhez való fizikai hozzáférést;
b) védi a fizikai létesítményt, biztosítja a rendszerhez szükséges infrastruktúrát;
c) biztosítja a rendszerhez szükséges háttér és kiegészítő szolgáltatásokat;
d) védi az informatikai rendszert a környezeti veszélyektől;
e) megfelelő környezeti intézkedésekről gondoskodik a rendszernek helyt adó létesítményekben.

A.Personnel_Security

A rendszer működtetője és üzemeltetője

a) biztosítja, hogy a szervezeten belül felelősségi körrel, feladattal rendelkező személyek megbízhatóak és megfelelnek az adott pozícióra vonatkozó biztonsági kritériumoknak;
b) biztosítja, hogy a rendszer üzemeltetői, belső felhasználói betartják a szervezeti biztonsági szabályokat, követik az érvényben lévő eljárásokat;
c) biztosítja, hogy a szervezeti információk és informatikai rendszerek védve legyenek a személyzeti mozgások esetére, így például egy felhasználó munkaköréből való eltávolítása vagy áthelyezése esetén.

[1] A: Assumptions (feltételezések), a jelölések megfelelnek a MIBÉTS módszertan alapját képező Common Criteria nemzetközi értékelési módszertan jelöléseinek.

A.Awareness_and_Training

A rendszer működtetője és üzemeltetője

a) biztosítja hogy az informatikai rendszer irányítói és a nem publikus alkalmazások felhasználói tudatában legyenek a tevékenységeikkel kapcsolatos biztonsági kockázatokkal, valamint az informatikai rendszerre vonatkozó törvényekkel, jogszabályi előírásokkal, szabványokkal, szabályzatokkal és eljárásokkal;
b) biztosítja, hogy a szervezet személyi állománya megfelelő képzésben részesüljön a számukra kijelölt, biztonsággal kapcsolatos feladatok és felelősségek teljesítése érdekében, továbbá amíg az üzemeltetés nem rendelkezik kellő gyakorlattal, ismerettel, (a biztonsági szabályok adta kereteken belül) az éles rendszer üzemeltetését támogassák a fejlesztők/integrátorok.

A.Media Protection

A rendszer működtetője és üzemeltetője a biztonsági szempontból érzékeny rendszerelemek, információk tekintetében

a) védi a szervezetnél fellelhető nyomtatott formájú vagy digitális adathordozón lévő információit;
b) jogosult felhasználókra korlátozza a célrendszerből kivett nyomtatott vagy digitális információkhoz való hozzáférést;
c) törli a digitális adathordozókat azok eltávolítása vagy újra használata előtt.

A rendszer életciklusában a biztonság elvárások teljesítésének folyamatos fenntartásához szükséges, hogy rendszer működtetője és üzemeltetője

- a szükséges változtatások során fenntartsa a rendszer értékelés idején fennálló biztonsági szintjét, az üzemeltetési dokumentációkat aktualizálja;
- fejlessze a biztonsági megoldásokat az Értékelési jelentésben szereplő biztonságnövelő javaslatok figyelembe vételével;
- időszakosan vizsgáltassa felül a rendszer biztonságát.

3. számú melléklet

A tanúsítással és értékeléssel kapcsolatos hivatkozások

Módszertani hivatkozások:

[M1]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v4 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M2]: Útmutató rendszer értékelőknek (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M3]: Útmutató rendszer tanúsítóknak (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M4]: IT biztonsági műszaki követelmények a különböző biztonsági szintekre - Követelmény előírás (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1.01, 2008.08.22) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M5]: NIST SP 800-53: National Institute of Standard and Technology U.S. Department of Commerce Specila Publications 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, February 2012

A tanúsításhoz felhasznált főbb dokumentumok és megalapozó értékelési jelentések azonosítása

3.1 Főbb dokumentumok:

[D1]: Hivatalos lapkiadási rendszer (WMS+PUB v1.0) - Rendszerbiztonsági előirányzat (SST v1.0), WMS+PUB_v1.2_rendszer_biztonsagi_eloiranyzat

[D2]: Hivatalos lapkiadási rendszer (WMS+PUB v1.0) Rendszer értékelési jelentés (WMS+PUB_SETR_v10)

[D3]: Hivatalos lapkiadási rendszer HUNG-T-MIBÉTS-06-2013 Tanúsítvány