Adatbázisok anonimizált összekapcsolását megvalósító rendszer (DBCS)

Rendszer biztonsági előirányzat

Verzió:	v1.0
Dátum:	2009.02.16.
Megrendelő:	Neumann János Digitális Könyvtár és Multimédia Központ KHT (NKHT)
Fájl:	DBCS_SST_v10.pdf
Minősítés:	Nyilvános
Oldalak:	52

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás
0.1	2008.11.12.	A szerkezet felállítása
0.5	2008.11.24.	Kiegészített változat
0.6	2008.12.07.	Előzetes értékelői vélemények alapján módosított változat
0.7	2008.12.14.	A biztonsági követelmények átírása a „fokozott kihatású biztonsági osztályokra” meghatározott követelmények alapján
0.8	2008.12.22.	Az előzetes értékelés (DBCS_ASST_ER_v02.doc) megállapításai alapján kiegészített és pontosított változat
0.9	2008.12.27.	A második értékelés (DBCS_ASST_ER_v03.doc) megállapításai alapján kiegészített és pontosított változat
0.91	2009.01.14.	A2009.01.13-i megbeszélés alapján kiegészített és pontosított változat, mely véleményezésre átadásra került a tanúsítónak.
0.92	2009.01.19.	A 2007. CI. törvény alapján történő összekapcsolására vonatkozó megállapodás I. sz. melléklete alapján pontosított változat
0.93	2009.01.23	A tanúsító véleményét beépítő változat, mely egyeztetésre átadásra került a megbízónak.
0.94	2009.01.27	A tervezési dokumentációk értékelése alapján pontosított változat.
1.0	2009.02.16	A megbízó véleményét és a teljes folyamat auditálásáról készült jelentést is figyelembe vevő, az értékeléshez véglegesnek tekintett változat.

Dokumentum információk:

Készült:	2009.02.16.
Készítette:	Balázs István
Átnézte:	Staub Klára

1. A rendszer egészének jellemzése

1.1 Bevezetés

1.1.1 SST hivatkozás

Jelen rendszer biztonsági előirányzat (SST) hivatkozása az alábbi:

Cím: **Anonimizált adatbázisok összekapcsolását megvalósító rendszer** – rendszer biztonsági előirányzat

Verzió: v1.0

Dátum: 2009.02.16.

1.1.2 STOE hivatkozás

A jelen SST az alábbi rendszer értékelés tárgyára (STOE) vonatkozik:

Név: **Anonimizált adatbázisok összekapcsolását megvalósító rendszer**

Rövid név: **DBCS (Data Base Connection System)**

Verzió: v1.0

1.1.3 A DBCS áttekintése

A DBCS egy olyan informatikai rendszer, mely anonim kapcsolati kód alkalmazásával lehetővé teszi különböző adatkezelők által kezelt személyes adatok és egyedi statisztikai adatok olyan összekapcsolását, mely biztosítja, hogy az összekapcsolt adatok az érintettekkel ne legyenek utólag kapcsolatba hozhatók.

A DBCS egy védett környezetben működtetett off-line (hálózatra nem kötött) rendszer, melyben két célszoftvert működtethet az erre felhatalmazott rendszerüzemeltető:

- az első célszoftver egy egyedi, véletlenszerűen megállapított elemeket is tartalmazó anonim kapcsolati kódképzési módszert (hash) állít elő a külső adatkezelők számára (rgen).
- a másik célszoftver az adatkezelők által az egyedi hash függvény felhasználásával anonimizált adatokat összekapcsolja, adatbázisba szervezi (dbcs).

A DBCS a fentieket az [1] és [2] elvárásainak megfelelő módon hajtja végre.

1.1.4 A DBCS leírása

A DBCS egy védett környezetben működtetett, hálózatra nem kötött rendszer, ahogyan azt az 1. ábra szemlélteti. A rendszer felhasználásra kész formában elkészíti az anonim kapcsolati kód képzését megvalósító programot, s ezt egy mobil adathordozón átadja az adatkezelőknek.

Szintén fizikai adathordozón kapja meg a rendszer az adatkezelőktől az előkészített, kapcsolati kódokkal ellátott, anonimizált adatállományokat. A rendszer az alábbi fő lépésekben feldolgozza ezeket:

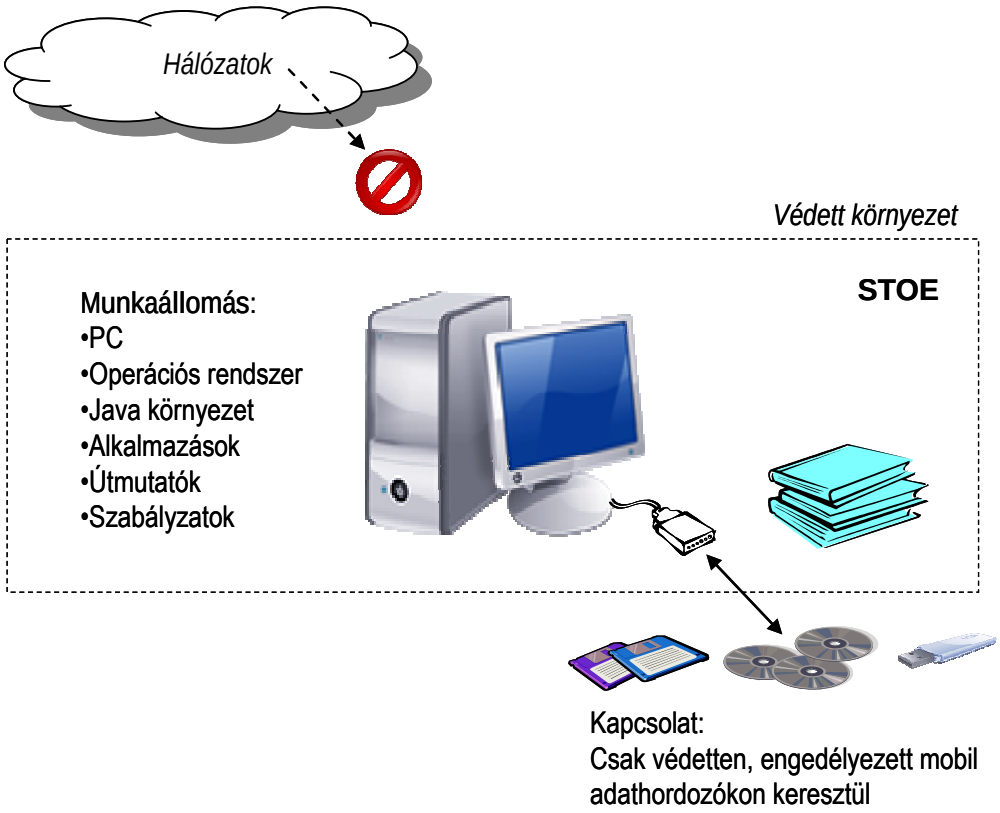
- az azonos kapcsolati kódokhoz tartozó adatok összekapcsolása,
- az összekapcsolt adatok adatbázisba szervezése,
- a kapcsolati kódok törlése,
- az összekapcsolt adatokat tartalmazó adatbázis adathordozóra írása.

Az eredményt tartalmazó adathordozó adatkérőnek történő védett átadásával a feladat lezárult.

1.1.4.1 A fizikai hatókör és határok áttekintése

A munkaállomás egy fizikai-környezetbiztonsági, valamint szabályozási-eljárásrendi szempontokból védett irodai környezetben helyezkedik el.

Az 1. ábra a munkaállomás legfontosabb fizikai elemeit és ezek kapcsolódásait részletezi.



1. ábra: A DBCS rendszer (STOE) fizikai elemei

A munkaállomás legfontosabb fizikai komponensei az alábbiak:

- egy beépített háttértároló és hálózati kapcsolat nélküli munkaállomás (az 1. ábrán a PC), mely a hardver alapokat biztosítja,
- egy pendrive, mely az alábbiak mesterpéldányát tartalmazza:
  - operációs rendszer (Linux, Ubuntu 8.10, Desktop i386),
  - JAVA futtató környezet (JRE v1.4.2),
- egy pendrive, mely az alábbiak mesterpéldányát tartalmazza:
  - hash-függvény készlet, melynek minden eleme egy anonim kapcsolati kód előállításra alkalmas hash függvény (hash),
  - véletlen generáló program készlet, melynek minden eleme egy hash függvényhez generál véletlen paramétereket (rgen),
  - adatbázis tételeket összekapcsoló program készlet, melynek minden eleme egy összekapcsolást megvalósító program (dbcs),
- egy live-CD (Ubuntu 8.10) operációs rendszert tartalmazó CD,
- egy munkapéldány pendrive, mely az alábbi mesterpéldányok másolatait tartalmazza:
  - operációs rendszer (Linux, Ubuntu 8.10, Desktop i386),
  - JAVA futtató környezet (JRE v1.4.2),
  - egy kiválasztott hash függvény (hash),
  - egy kiválasztott véletlen generáló program (rgen),

- egy kiválasztott összekapcsoló program (dbcs),

- Útmutatók, melyek segítségével elvégezhetők a fenti hardver és szoftver komponensek biztonságos telepítése, konfigurálása és üzemeltetése.
- Szabályzatok, melyek a biztonságos üzemeltetés elvárásait fogalmazzák meg.

Valamennyi fenti komponens az STOE részét képezi.

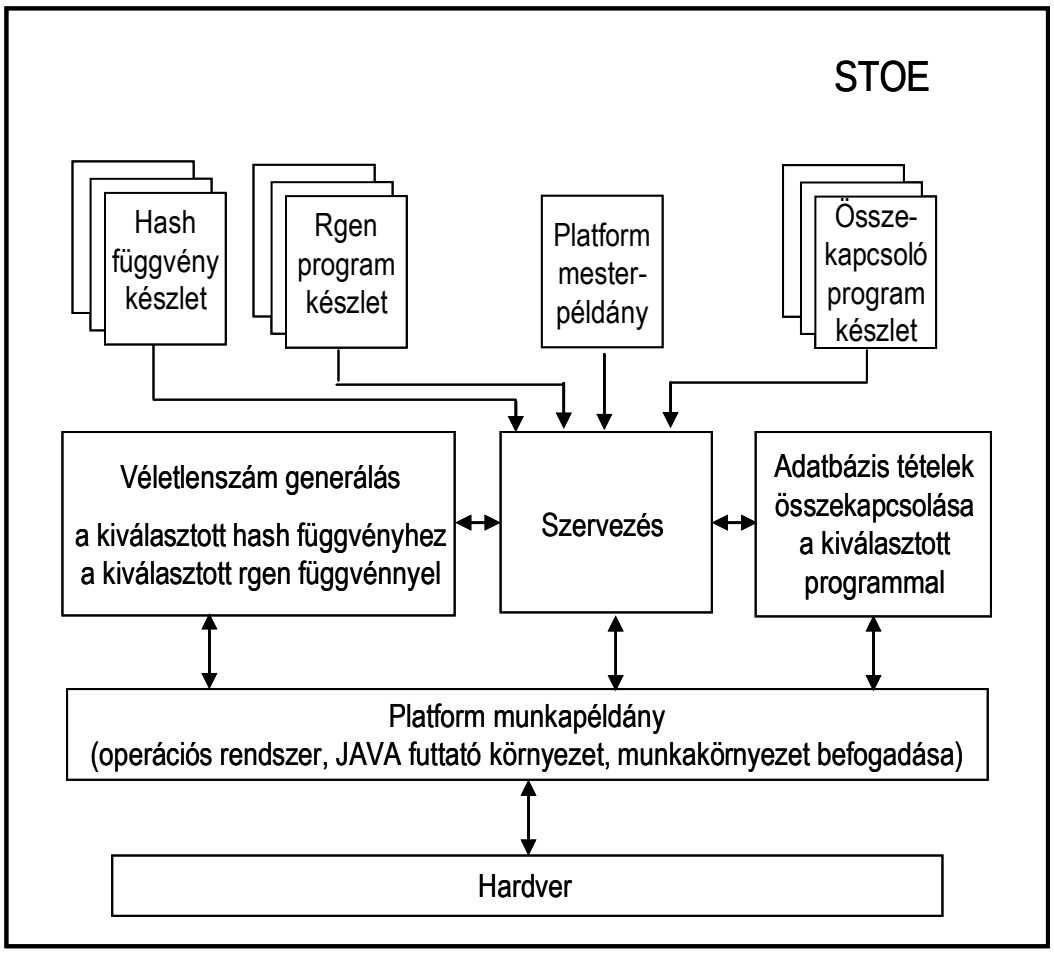
A munkaállomás valamennyi fizikai komponensét megadtuk.

A munkaállomás más komponenst nem tartalmazhat.

1.1.4.2 A logikai hatókör és határok áttekintése

A DBCS rendszerben különböző szolgáltatások nyújtása, illetve igénybe vétele folyik.

A 2. ábra a logikai alrendszerek egymáshoz kapcsolódását tekinti át:



2. ábra: A DBCS logikai alrendszerei és egymáshoz kapcsolódásuk

A **platform** alrendszer megbízható futtatási környezetet biztosít a többi alrendszer számára, egyúttal naplózza a hatókörébe eső, biztonsági szempontból fontos eseményeket. A biztonságos futtatási környezet több biztonsági funkciót megvalósít:

- tartomány szétválasztást (a különböző alrendszerek egymást nem befolyásolhatják, egymás erőforrásait nem érik el),
- önvédelmet (megvédi a különböző alrendszereket a jogosulatlan logikai hozzáféréstől)

- megkerülhetetlenséget (a többi alrendszer csak akkor éri el erőforrásait, ha az operációs rendszerbe belépő, megfelelő jogosultságú felhasználó - a rendszerüzemeltető - elindítja azokat).

A DBCS fejlesztése előállította a munkaállomás hardverkörnyezetére hangolt olyan operációs rendszer mesterpéldányát, amely képes CD/DVD-t írni és olvasni, JAVA-t futtatni, és nem igényel nagy hardverkapacitást (egyszerű grafikájú, kis méretű, kevés memóriát foglaló).

Minden adatkéréshez egy egyedi adat-összekapcsolást megvalósító projekt tartozik. Minden projekt egy platform munkapéldány pendrive-on valósul meg, amelynek tartalma kezdetben üres, a szervezés alrendszer tölti fel és kezeli a következőkben részletezett módon.

A **szervezés** alrendszer (mely egy live-CD (Ubuntu 8.10) operációs rendszerből, egy ellenőrző összeg számító alkalmazásból áll) létrehozza a platform munkapéldányt a mesterpéldányból, kiválasztja a megfelelő készletből az aktuális hash függvényt, rgen függvényt és összekapcsoló programot, különböző input/output műveleteket közvetít, végül törli a munkapéldányokat tartalmazó pendrive teljes tartalmát.

A **véletlenszám generálás** alrendszer a kiválasztott hash függvényhez véletlen paramétereket generál, egyúttal naplózza a hatókörébe eső, biztonsági szempontból fontos eseményeket.

Az **adatbázis tételek összekapcsolása** alrendszer a kiválasztott összekapcsoló programmal az adatkezelőktől kapott (anonimizált) adatbázis tételeket kapcsolja össze, egyúttal naplózza a hatókörébe eső, biztonsági szempontból fontos eseményeket.

Valamennyi fenti szolgáltatás az STOE részét képezi.

A rendszer valamennyi szolgáltatását megadtuk.

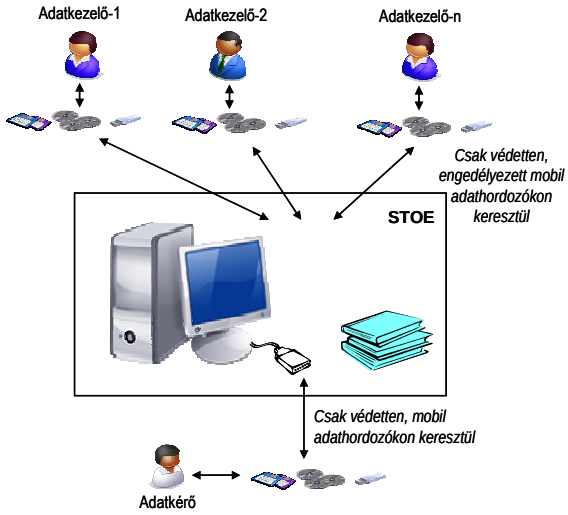
1.1.4.3 A DBCS külső rendszerekhez kapcsolódása

A DBCS több külső informatikai rendszerhez is kapcsolódik, melyet a 3. ábra szemléltet:

- **Adatkérő** (informatikai rendszere), melynek rendszerbeli feladatai az alábbiak:
  - az adatkérés céljának, valamint az ennek megfelelő célsokaság meghatározása (milyen alanyok mely adataira van szüksége),
  - a kiválasztási szempontok és a reprezentativitást igénylő ismérvek megadása,
  - az összekapcsolás alapját képező egyedi azonosító elem meghatározása.
- **Mintaképzésért felelős adatkezelő** (informatikai rendszere), melynek rendszerbeli feladatai:
  - mintavételezés az adatkérő által meghatározottak alapján,
  - anonim kapcsolati kód előállítása (a mintavételezés után előállt tételekben az összekapcsolás alapját képező azonosítóra számolva) a DBCS-től kapott, az anonim kapcsolati kód képzését megvalósító programmal,
  - egy kizárólag az anonim kapcsolati kódokat tartalmazó lista összeállítása és DBCS-hez továbbítása,
  - a mintavételezés után előállt tételek (bennük az anonim kapcsolati kódokkal) összeállítása és DBCS-hez továbbítása.
- **Kapcsolódó adatkezelő**(k) (informatikai rendszere), mely(ek)nek rendszerbeli feladata az alábbi:
  - mintához igazodó leválogatás saját adatbázisában, a DBCS-től kapott, anonim kapcsolati kódokat tartalmazó lista alapján,
  - a kapott tétellista szűkítése (amennyiben az adatkérő olyan kiválasztási és reprezentativitási feltételeket is meghatározott, melyek rá vonatkoznak),
  - a leválogatás és az opcionális szűkítés után előállt tételek (bennük az anonim kapcsolati kódokkal) összeállítása és DBCS-hez továbbítása.

Valamennyi külső informatikai rendszerhez kapcsolódás (pontosabban annak DBCS oldali interfésze) az STOE részét képezi.

A DBCS rendszer valamennyi külső kapcsolódását megadtuk.



3. ábra: A DBCS rendszer kapcsolódása külső rendszerekhez

1.1.5 Tartomány kialakítás specifikáció

A DBCS egységes biztonsági tartományt képvisel (nem osztható olyan különböző biztonsági tartományokra, melyek üzemeltetési környezetében jelentős eltérések lennének).

1.2 Megfelelőségi nyilatkozatok

1.2.1 A megfelelőségi nyilatkozat tartalma

Jelen rendszer biztonsági előirányzat, s az általa vizsgált DBCS rendszer az alábbi mértékadó dokumentumhoz való megfelelőséget állít:

- ***[8]: IT biztonsági műszaki követelmények a különböző biztonsági szintekre, BME IK, 2008.***

A [8]-ben leírt „fokozott kihatású biztonsági osztály követelményei” biztonsági követelmény csomagra vonatkozó csomag-megfelelőség: „***módosítja a fokozott kihatású biztonsági osztály követelményeit***”.

A módosítás ellenére a DBCS teljesíti a [8]-ben leírt „fokozott kihatású biztonsági osztály követelményei” biztonsági követelmény csomag valamennyi elvárását (tehát bővítésről van szó).

A DBCS ugyanakkor figyelembe veszi az alábbi jogszabályokban megfogalmazott elvárásokat is:

- [1]: 2007. évi CI. törvény 4.-8. §-ai,
- [2]: 335/2007. (XII. 13.) kormányrendelet 1. és 9. §-ai.

1.2.2 A megfelelőségi nyilatkozat indoklása

1.2.2.1 Jogszabályokban megfogalmaznak elvárások

Az indoklás előkészítéseként tekintsük át a DBCS rendszerre jogszabályokban megfogalmaznak elvárásokat.

Az [1] törvény a rendszertől elvárt funkcionalitást az alábbi módon határozza meg:

4 §

(1) A miniszter és a kormányhivatal vezetője kérheti, hogy egyes, személyes adatot vagy egyedi statisztikai adatot adóazonosító jellel, társadalombiztosítási azonosító jellel, személyazonosító jellel, vagy névvel és lakcímmel együtt kezelő költségvetési szervek adatbázis készítésére alkalmas módon adják át az alanyával kapcsolatba nem hozható, a 2. § szerint módosított adatot.

(2) Az (1) bekezdés szerinti adatátadást az adatbázis létrehozásáért felelős szerv részére, az általa megállapított kódképzési módszer alapján meghatározott anonim kapcsolati kóddal és mintavételi eljárással kell teljesíteni.

(3) Az adatok összekapcsolását az adatbázis létrehozásáért felelős szerv végzi oly módon, hogy a különböző adatkezelőktől azonos módszerrel képzett kapcsolati kóddal veszi át az adatokat.

(4) Adatok összekapcsolásával létrehozott adatbázis esetén az anonim kapcsolati kód képzésének módszerét úgy kell meghatározni, hogy az alapját képező személyazonosító adatok kezelésére valamennyi, az adatátadás céljából megkeresett adatkezelő jogosult legyen.

(5) Az adatbázis létrehozásáért felelős szerv kérésére az egyik adatkezelő szerv mintát vesz az általa kezelt adatbázisból, és annak kapcsolati kódjait átadja az adatbázis létrehozásáért felelős szervnek.

(6) Az adatbázis létrehozásáért felelős szerv az (5) bekezdés szerinti minta anonim kapcsolati kódjait, az ehhez tartozó adatok nélkül átadja az (1) bekezdés szerinti adatkérésben megjelölt többi adatkezelőnek.

5 §

(1) Az anonim kapcsolati kód képzésének módszerét és a kódképzés alapját az adatbázis létrehozásáért felelős szerv úgy határozza meg, hogy

a) a kódképzés alapját nem képezhetik olyan személyazonosító adatok, amelyek kezelésére az adatkérő jogosult,

b) a kódképzés alapját nem képezhetik olyan személyazonosító adatok, amelyek kezelésére az adatbázis létrehozásáért felelős szerv jogosult,

c) a kódképzés konkrét módszere tartalmazzon egyedi, véletlenszerűen megállapított elemet.

(2) Az adatbázis létrehozásáért felelős szerv a kódképzés módszerét csak az adatkezelő szerveknek továbbíthatja. A továbbítás után a kódképzés módszerét haladéktalanul törölni kell.

(5) Az adatbázis létrehozásáért felelős szerv az adatátadásra 5 napos időintervallumot határoz meg. Az ezen időintervallumon kívül érkezett adatokat a többi adattal össze nem kapcsolhatja, azok kapcsolati kódját haladéktalanul törli.

(6) Az adatbázis létrehozásáért felelős szervnek az összekapcsolást követően az anonim kapcsolati kód és az átvett adatok közötti kapcsolatot helyreállíthatatlanul meg kell szüntetnie és az anonim kapcsolati kódot haladéktalanul törölnie kell.

6 §

(1) Az adatbázis létrehozásáért felelős szerv tevékenységét, az adatigénylés, adatátadás és adat-összekapcsolás jogszerűségét és az anonim kapcsolati kód képzésének módszerét az adatvédelmi biztos a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvényben meghatározott eljárásban előzetesen is ellenőrizheti.

7 §

(1) …, a 4. § szerinti kapcsolás esetén az adatbázis létrehozásáért felelős szerv az adatok átadása előtt a természetes személy lakcímére vonatkozó adatot úgy módosítja, hogy abból az érintett lakóhelye a kistérségnél pontosabban ne legyen megállapítható.

(2) … a 4. § szerinti adatátadás esetében adatkezelőnként legalább száz főt eredményező mintát kell venni. A teljes népességre vonatkozó adatbázisok esetében a minta nem haladhatja meg a teljes sokaság 50%-át.

(3) Az adatbázis létrehozásáért felelős szerv az (1) bekezdés szerinti művelet elvégzése után az adatbázist megküldi a 4. § (1) bekezdése szerinti adatkérőnek.

(4) Az adatbázis létrehozásáért felelős szerv honlapján kereshető formában közzéteszi az adatkéréseket: az adatkör leírását, kezelőit, a 2. § (1) és a 4. § (1) bekezdése szerinti adatkérő megnevezését, valamint az adatkérés és a megtagadás vagy a teljesítés dátumát.

(5) A 2. § (1) bekezdése és a 4. § (1) bekezdése szerinti adatátadás az adatkérő által irányított vagy felügyelt költségvetési szerv részére is történhet.

8 §

(1) E törvény alkalmazásában

a) anonim kapcsolati kód: az ugyanazon személyre vonatkozó személyazonosító adatokból olyan, véletlenszerű elemet is tartalmazó módszerrel képzett karaktersor, amellyel ugyanazokból az adatokból mindig ugyanaz a karaktersor jön létre, de amely eredményeképpen létrejött karaktersorból a személyazonosító adatok nem állíthatók helyre;

b) kistérség: a települési önkormányzatok többcélú kistérségi társulásáról szóló törvény szerinti kistérség, Budapest esetében a kerület.

(2) Az e törvényben foglaltak nem alkalmazhatóak a külön törvény szerinti minősített adatokra, illetve azokra a közérdekű adatokra, amelyeknek megismerhetőségét nemzetbiztonsági érdekből külön törvény korlátozza.

A [2] rendelet az alábbi kiegészítő elvárásokat fogalmazza meg:

1 §

(1) A Kormány az adatbázis létrehozásáért felelős szervként a Neumann János Digitális Könyvtár és Multimédia Központ Kht.-t (a továbbiakban: NKHT) jelöli ki.

9 §

(2) Az NKHT az anonim kapcsolati kód képzésének módját programozott, felhasználásra kész formában adja meg az adatkezelőknek.

1.2.2.2 A rendszerre elvárt informatika biztonsági szint

Az alábbiakban a [9]-ben leírt biztonsági kategorizálás módszerével meghatározzuk a DBCS rendszerre elvárt informatika biztonsági szintet.

A DBCS rendszer által kezelt adatok között személyes adatok is lehetnek, egyben a személyes adatok képezik a legmagasabb védelmi szintet megkívánó információ típust. A személyes adatok **bizalmasság**ának sérülésével járó potenciális hatás mértéke (kihatás szint) **fokozott**, mert a bizalmasság elvesztése várhatóan komoly hátrányos hatást gyakorol az adatbázis összekapcsolásban érintett szervezetekre és a személyes adatok alanyaira.

A DBCS rendszer által kezelt adatok összekapcsolására jelentős társadalmi vagy gazdasági hatású, valamint különösen az európai uniós kötelezettségek teljesítését érintő döntések előkészítése érdekében kerül sor. Az összekapcsolandó adatok **sértetlenség**ének sérülésével járó potenciális hatás (kihatás szint) **fokozott**, mert a sértetlenség elvesztése komoly hátrányos hatást gyakorolhat az összekapcsolás eredményére.

A DBCS rendszer által kezelt adatok **rendelkezésre állás**ának sérülésével járó potenciális hatás (kihatás szint) **alacsony**, mert a rendelkezésre állás elvesztése várhatóan csak korlátozott hátrányos hatást gyakorol a döntés előkészítésre (hiszen ez csak a viszonylag ritkán esedékes adat-összekapcsolás elhalasztását, vagy kényszerű megismétlését okozná).

A fenti megállapítások az alábbi biztonsági kategóriát határozza meg:

BIZTONSÁGI KATEGÓRIA/kezelt személyes adatok =
{(bizalmasság, fokozott), (sértetlenség, fokozott), (rendelkezésre állás, alacsony)}

BIZTONSÁGI KATEGÓRIA/összekapcsolandó adatok =
{(bizalmasság, fokozott), (sértetlenség, fokozott), (rendelkezésre állás, alacsony)}

A biztonsági kategóriát a három biztonsági célra (bizalmasság, sértetlenség, rendelkezésre állás) és a különböző információ típusokra (kezelt személyes adatok, összekapcsolandó adatok) kapott legnagyobb kihatás határozza meg, ez pedig a DBCS esetén: **fokozott**.

1.2.2.3 A rendszerre vonatkozó speciális elvárások

A „fokozott kihatású biztonsági osztály” általános követelményei között nem szerepel néhány olyan elvárás, melyet az [1] és [2] jogszabályok megfogalmaztak. Ezért indokolt, hogy ezek bővítésként szerepeljenek a DBCS rendszer felvállalt követelményei között.

A módosított (kiegészítő) követelmények az alábbiak:

- SK-1 (Adatbázis elemek összekapcsolása)
- SK-2 (Minősített hash függvény)
- SK-3 (Véletlenített hash függvény)
- SK-4 (Visszaállíthatatlan törlés)

1.2.2.4 A kiegészítő követelmények visszavezetése a DBCS rendszer biztonsági céljaira

Az 1. táblázat a kiegészítő követelményeket visszavezeti a DBCS rendszerre vonatkozó biztonsági célokra.

kiegészítő követelmény **(részletezve 1.5.1.7 alatt)**	**a kiegészítő követelmény által támogatott biztonsági cél** **(részletezve 1.4.1 alatt)**
SK-1 (Adatbázis elemek összekapcsolása)	O1 (Az összekapcsolt adatok alanyának védelme)
SK-2 (Minősített hash függvény)	O1 (Az összekapcsolt adatok alanyának védelme)
SK-3 (Véletlenített hash függvény)	O2 (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása)
SK-4 (Visszaállíthatatlan törlés)	O2 (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása)

1. táblázat: A kiegészítő követelmények és a DBCS rendszerre vonatkozó biztonsági célok közötti megfeleltetés

Az 1. táblázat a 6. táblázatnak a kiegészítő követelményekre vonatkozó részét tartalmazza.

Az 1. táblázat visszavezetésének indoklása megtalálható a 6. táblázatot követő általánosabb indokláson belül (1.5.2 alatt).

1.3 Biztonsági probléma meghatározás

1.3.1 Fenyegetések

A DBCS rendszerre irányuló (kivédendő) fenyegetések az alábbiak:

T1 (Következtetés az adat alanyára)
Az összekapcsolt adatokból következtetéseket von le az adatok alanyára az adatkérő, az adatkezelő, az (összekapcsolást végző) adatbázis létrehozásáért felelős szerv, vagy kívülállók.

T2 (Kiterjesztett összekapcsolás)
Különböző adat összekapcsolásokból származó eredményeket ismételten összekapcsol az adatkérő, az adatkezelő, az adatbázis létrehozásáért felelős szerv, vagy kívülállók.

1.3.2 Szervezeti biztonsági szabályok

Nincsenek szervezeti biztonsági szabályok.

1.3.3 A DBCS üzemeltetési környezetére vonatkozó feltételezések

A DBCS rendszer üzemeltetési környezetére vonatkozó feltételezések az alábbiak:

A1 (Fizikai védelem)
A környezet megfelelő fizikai védelmet biztosít, mely garantálja, hogy a rendszer komponenseit (köztük a különböző alkalmazásokat és ezek konfigurációs állományait) nem lehet módosítani, valamint a rendszerben generált érzékeny adatokat (a hash függvényhez generált véletlen értékeket) illetéktelenül nem lehet megismerni.

A2 (Helyes telepítés és konfigurálás)
A rendszer valamennyi komponensét úgy telepítik és konfigurálják, hogy biztonságos állapotban kezd el üzemelni.

A3 (Megbízható rendszeradminisztrátor)
A rendszeradminisztrátor ismeri feladatait, s ezeket szakképzett módon, lehetőségeivel nem visszaélve látja el.

A4 (Felhatalmazott rendszerüzemeltető)
Az engedéllyel rendelkező felhasználó megbízható a tekintetben, hogy a számára kijelölt feladatokat biztonsági szempontból korrekt módon hajtja végre.

A5 (Megbízható rendszervizsgáló)
A biztonsági naplókat (a DBCS rendszeren kívül) áttekintő és kezelő rendszervizsgáló ismeri feladatait, s ezeket szakképzett módon, lehetőségeivel nem visszaélve látja el.

A6 (Megbízható szállítás)
A DBCS rendszer valamennyi külső informatikai rendszerhez kapcsolódását biztosító adathordozó szállítása (küldés és fogadás egyaránt) védett módon, az adathordozón tárolt adatok sértetlenségének és bizalmasságának megőrzését biztosítva történik.

1.4 Biztonsági célok

1.4.1 A DBCS rendszerre vonatkozó biztonsági célok

Az [1] törvény és a [2] kormányrendelet az alábbi magas szintű biztonsági elvárásokat (biztonsági értékeléssel ellenőrizendő biztonsági célokat) határozza meg a rendszerre:

O1 (Az összekapcsolt adatok alanyának védelme)
Az összekapcsolt adatokból ne következtethessen az adatok alanyára sem egy kívülálló, sem az alábbiak egyike: adatkérő, adatkezelő, az (összekapcsolást végző) adatbázis létrehozásáért felelős szerv.

O2 (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása)
Különböző adat összekapcsolásokból származó eredményeket ismételten ne kapcsolhasson össze sem egy kívülálló, sem az alábbiak egyike: adatkérő, adatkezelő, az (összekapcsolásokat végző) adatbázis létrehozásáért felelős szerv.

1.4.2 Az üzemeltetési környezetre vonatkozó biztonsági célok

A DBCS rendszer üzemeltetési környezetére az alábbi (auditálással ellenőrizendő) általános biztonsági célok vonatkoznak:

OE1 (Fizikai védelem)
A környezetnek olyan szintű fizikai védelemről kell gondoskodnia, mely garantálja, hogy a rendszer komponenseit (köztük a különböző alkalmazásokat és ezek konfigurációs állományait) ne lehessen módosítani, valamint a rendszerben generált érzékeny adatokat (a hash függvényhez generált véletlen értékeket) ne lehessen illetéktelenül megismerni.

OE2 (Helyes telepítés és konfigurálás)
A rendszer valamennyi komponensét úgy kell telepíteni és konfigurálni, hogy biztonságos állapotban kezdjen el üzemelni.

OE3 (Megbízható rendszeradminisztrátor)
A rendszeradminisztrátor ismerje feladatait, s ezeket szakképzett módon, lehetőségeivel nem visszaélve lássa el.

OE4 (Felhatalmazott rendszerüzemeltető)
Az engedéllyel rendelkező felhasználó legyen megbízható a tekintetben, hogy a számára kijelölt feladatokat biztonsági szempontból korrekt módon hajtja végre.

OE5 (Megbízható rendszervizsgáló)
A biztonsági naplókat (a DBCS rendszeren kívül) áttekintő és kezelő rendszervizsgáló ismerje feladatait, s ezeket szakképzett módon, lehetőségeivel nem visszaélve lássa el.

OE6 (Megbízható szállítás)
A DBCS rendszer valamennyi külső informatikai rendszerhez kapcsolódását biztosító adathordozó szállítása (küldés és fogadás egyaránt) védett módon, az adathordozón tárolt adatok sértetlenségének és bizalmasságának megőrzését biztosítva történjen.

Megjegyzés: A DBCS rendszerre és annak üzemeltetési környezetére vonatkozó fenti biztonsági célokat az adatbázis létrehozásáért felelős szerv (NKHT) műszaki, üzemeltetési és menedzsment intézkedésekkel valósíthatja meg.

1.4.3 A biztonsági célok indoklása

A 2. táblázat a DBCS rendszerre vonatkozó biztonsági célokat visszavezeti a biztonsági célok által kivédett fenyegetésekre:

a DBCS rendszerre vonatkozó biztonsági cél	a biztonsági cél által kivédett fenyegetés
O1 (Az összekapcsolt adatok alanyának védelme)	T1 (Következtetés az adat alanyára)
O2 (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása)	T2 (Kiterjesztett összekapcsolás)

2. táblázat: A DBCS rendszerre vonatkozó biztonsági célok és az általuk kivédett fenyegetések

A 3. táblázat a DBCS rendszer üzemeltetési környezetére vonatkozó biztonsági célokat visszavezeti az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által támasztott feltételezésekre:

az üzemeltetési környezetre vonatkozó biztonsági cél	a biztonsági cél által kivédett fenyegetés/támasztott feltétel
OE1 (Fizikai védelem)	T1 (Következtetés az adat alanyára) T2 (Kiterjesztett összekapcsolás) A1 (Fizikai védelem)
OE2 (Helyes telepítés és konfigurálás)	T1 (Következtetés az adat alanyára) T2 (Kiterjesztett összekapcsolás) A2 (Helyes telepítés és konfigurálás)
OE3 (Megbízható rendszeradminisztrátor)	A3 (Megbízható rendszeradminisztrátor)
OE4 (Felhatalmazott rendszerüzemeltető)	A4 (Felhatalmazott rendszerüzemeltető)
OE5 (Megbízható rendszervizsgáló)	A5 (Megbízható rendszervizsgáló)
OE6 (Megbízható szállítás)	A6 (Megbízható szállítás)

3. táblázat: A DBCS rendszer üzemeltetési környezetésre vonatkozó biztonsági célok és az általuk kivédett fenyegetések és támasztott feltételek

A 4. táblázat a fenyegetéseket és a kivédésükben közreműködő biztonsági célokat mutatja.

fenyegetés	biztonsági cél
T1 (Következtetés az adat alanyára)	O1 (Az összekapcsolt adatok alanyának védelme) OE1 (Fizikai védelem) OE2 (Helyes telepítés és konfigurálás)
T2 (Kiterjesztett összekapcsolás)	O2 (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása) OE1 (Fizikai védelem) OE2 (Helyes telepítés és konfigurálás)

4. táblázat: A fenyegetések és a biztonsági célok közötti megfeleltetés

A 2. táblázat mutatja, hogy minden DBCS rendszerre vonatkozó biztonsági cél (O1, O2) szükséges, ténylegesen hozzájárul legalább egy fenyegetés kivédéséhez (elhárításához, csökkentéséhez vagy a következmények csillapításához).

A 3. táblázat mutatja, hogy minden üzemeltetési környezetre vonatkozó biztonsági cél (OE1 – OE6) szükséges, ténylegesen hozzájárul legalább egy fenyegetés kivédéséhez, vagy egy feltételezés alátámasztására.

A 4. táblázat mutatja, hogy minden fenyegetésre (T1, T2) van ennek kivédését támogató biztonsági cél.

A T1 fenyegetést elhárítják:

- Az O1 (DBCS-re vonatkozó) biztonsági cél közvetlenül a T1 fenyegetés kivédésére irányul.
- Az OE1 (üzemeltetési környezetre vonatkozó) biztonsági cél hozzájárul a T1 fenyegetés kivédéséhez, mivel (fizikai védelemmel) azt garantálja, hogy az O1-t megvalósító műszaki intézkedéseket nem lehet lerontani, meghamisítani.
- Az OE2 (üzemeltetési környezetre vonatkozó) biztonsági cél is hozzájárul a T1 fenyegetés kivédéséhez, mivel (helyes telepítéssel és konfigurálással) azt garantálja, hogy az O1-t megvalósító műszaki intézkedések megfelelően működnek.

A T2 fenyegetést elhárítják:

- Az O2 (DBCS-re vonatkozó) biztonsági cél közvetlenül a T2 fenyegetés kivédésére irányul.
- Az OE1 (üzemeltetési környezetre vonatkozó) biztonsági cél hozzájárul a T2 fenyegetés kivédéséhez, mivel (fizikai védelemmel) azt garantálja, hogy az O2-t megvalósító műszaki intézkedéseket nem lehet lerontani, meghamisítani.
- Az OE2 (üzemeltetési környezetre vonatkozó) biztonsági cél is hozzájárul a T2 fenyegetés kivédéséhez, mivel (helyes telepítéssel és konfigurálással) azt garantálja, hogy az O2-t megvalósító műszaki intézkedések megfelelően működnek.

Az 5. táblázat az üzemeltetési környezetre vonatkozó feltételezéseket és az alátámasztásukban közreműködő (üzemeltetési környezetre vonatkozó) biztonsági célokat mutatja.

az üzemeltetési környezetre vonatkozó feltételezés	**az üzemeltetési környezetre vonatkozó biztonsági cél**
A1 (Fizikai védelem)	OE1 (Fizikai védelem)
A2 (Helyes telepítés és konfigurálás)	OE2 (Helyes telepítés és konfigurálás)
A3 (Megbízható rendszeradminisztrátor)	OE3 (Megbízható rendszeradminisztrátor)
A4 (Felhatalmazott rendszerüzemeltető)	OE4 (Felhatalmazott rendszerüzemeltető)
A5 (Megbízható rendszervizsgáló)	OE5 (Megbízható rendszervizsgáló)
A6 (Megbízható szállítás)	OE6 (Megbízható szállítás)

5. táblázat: A feltételezések és a biztonsági célok közötti megfeleltetés

Az 5. táblázat mutatja, hogy valamennyi feltételezést alátámasztják:

- az OE1 biztonsági cél közvetlenül alátámasztja az A1 feltételezést,
- az OE2 biztonsági cél közvetlenül alátámasztja az A2 feltételezést,
- az OE3 biztonsági cél közvetlenül alátámasztja az A3 feltételezést,
- az OE4 biztonsági cél közvetlenül alátámasztja az A4 feltételezést,
- az OE5 biztonsági cél közvetlenül alátámasztja az A5 feltételezést,
- az OE6 biztonsági cél közvetlenül alátámasztja az A6 feltételezést.

1.5 Biztonsági követelmények

1.5.1 A rendszer által felvállalt biztonsági követelmények

1.2.2.2 pont indoklása alapján a DBCS rendszerre a fokozott kihatású biztonsági osztály követelményeit alkalmazni kell, melyet esetleg speciális elvárások egészíthetnek ki (lásd az 1.5.1.7 pont alatti SK-1 - SK-4 követelményeket).

A fokozott kihatású biztonsági osztályra vonatkozó alábbi informatika biztonsági műszaki követelményeket a [8] határozta meg. A dőlt betűtípussal szedett részek az általánosan megfogalmazott követelmények testre szabását jelzik, a kijelölt műveletek elvégzésével.

1.5.1.1 Azonosítás és hitelesítés (AH)

AH-1 Azonosítási és hitelesítési szabályzat és eljárásrend
A szervezet kifejleszt, terjeszt, rendszeresen felülvizsgál és frissít:

- egy formális, dokumentált, azonosításra és hitelesítésre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettség, koordináció a szervezet egységei között, megfelelés, illetve
- egy formális, dokumentált eljárásrendet, amelynek célja az azonosításra és hitelesítésre vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

AH-2 Felhasználó azonosítása és hitelesítése
Az informatikai rendszer egyedileg azonosítja és hitelesíti a felhasználókat (vagy a felhasználók nevében eljáró eljárásokat)
(a) bővítés: Az informatikai rendszer többtényezős hitelesítést használ a távoli hozzáférésre, ami kriptográfiai kulcsbirtoklás bizonyításán alapul. A kriptográfiai kulcsot tárolhatja [értékadás: Szoftver token, FIPS 140-2 1-es szinten tanúsított hardver; vagy FIPS 140-2 2-es vagy magasabb szinten tanúsított hardver.]

Megjegyzés: A DBCS rendszer nem tesz lehetővé távoli hozzáférést, következésképp az (a) bővítésben megfogalmazott követelmény automatikusan teljesítettnek tekinthető.

AH-3 Eszközök azonosítása és hitelesítése
Az informatikai rendszer bizonyos eszközöket azonosít és hitelesít, mielőtt kapcsolatot létesítene velük.

AH-4 Azonosító kezelés
A szervezet az alábbi módon kezeli a felhasználói azonosítókat:

- egyedileg azonosít minden felhasználót;
- ellenőrzi minden felhasználó azonosságát;
- egy új felhasználói azonosító kibocsátását adminisztrátori felhatalmazáshoz köti;
- garantálja, hogy a felhasználói azonosítót annak a félnek adták ki, akinek szánták; és
- lezárja a felhasználói azonosítót egy *[5 munkanap]*-ig tartó inaktivitás után.

AH-5 A hitelesítésre szolgáló eszközök kezelése
A szervezet az alábbi módon kezeli a rendszer hitelesítésre szolgáló eszközeit:

- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;

- adminisztratív eljárásokat vezet be a hitelesítésre szolgáló eszközök kezdeti szétosztására, az elvesztett/kompromittálódott vagy sérült eszközök esetére, illetve a hitelesítésre szolgáló eszközök visszavonására;
- az alapértelmezés szerinti hitelesítésre szolgáló eszközöket megváltoztatja az informatikai rendszer installálásának során; és
- időszakonként a hitelesítésre szolgáló eszközöket megváltoztatja/frissíti.

AH-6 A hitelesítésre szolgáló eszköz visszacsatolása
Az informatikai rendszer visszacsatolást biztosít a felhasználónak hitelesítési kísérlete során, és ez a visszacsatolás nem veszélyezteti a hitelesítési mechanizmust. Az informatikai rendszer elrejti a hitelesítési információk visszacsatolását a hitelesítési kísérlet során, így védve az információt az esetleges kihasználástól/illetéktelen használattól.

AH-7 Hitelesítés kriptográfiai modul esetén
Az informatikai rendszer egy kriptográfiai modul hitelesítésére olyan hitelesítési módszereket használ, amelyek megfelelnek a törvényeknek, vezetői döntéseknek, direktíváknak, szabályzatoknak, előírásoknak, szabványoknak és útmutatóknak.

Megjegyzés: A DBCS rendszer nem alkalmaz kriptográfiai modult, következésképp az AH-7 követelmény automatikusan teljesítettnek tekinthető.

1.5.1.2 Hozzáférés ellenőrzése (HE)

HE-1 Hozzáférés ellenőrzési szabályzat és eljárásrend
A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:
- egy formális, dokumentált hozzáférés ellenőrzési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettség, koordináció a szervezet egységei között, megfelelés, illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a hozzáférés ellenőrzési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

HE-2 Felhasználói fiókok kezelése
A szervezet kezeli az informatikai rendszer felhasználói fiókjait, beleértve a felhasználói fiókok létrehozását, aktiválását, módosítását, felülvizsgálatát, letiltását és eltávolítását. A szervezet felülvizsgálja az informatikai rendszer felhasználói fiókjait [*minden adatbázis összekapcsolási projektben*].
(a) bővítés: A szervezet automatizált mechanizmusokat alkalmaz a felhasználói fiókok kezelésének támogatására.
(b) bővítés: Az informatikai rendszer automatikusan leállítja az ideiglenes és a kényszerhelyzetben létrehozott felhasználói fiókokat [értékadás: az egyes felhasználói fiók típusokra a szervezet által definiált időtartam] letelte után.
(c) bővítés: Az informatikai rendszer automatikusan letiltja az inaktív felhasználói fiókokat [*5 munkanap*] letelte után.
(d) bővítés: A szervezet automatikus mechanizmusokat használ a felhasználói fiókok kialakítására, módosítására, zárolására, visszavonására és egyes személyek szükség szerinti értesítésére.
Megjegyzés: A DBCS rendszer nem kezel ideiglenes és kényszerhelyzetben létrehozott felhasználói fiókokat, következésképp a (b) bővítésben megfogalmazott követelmény automatikusan teljesítettnek tekinthető.

Megjegyzés: Mivel a DBCS rendszer egyetlen munkaállomásból áll, se szükség, se lehetőség nincs központi hozzáférés kezelésre. Következésképp a (d) bővítésben megfogalmazott követelmény automatikusan teljesítettnek tekinthető.

HE-3 Hozzáférés ellenőrzés érvényre juttatása
Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszerhez való hozzáférés ellenőrzéséhez.
(a) bővítés: Az informatikai rendszer biztosítja, hogy a biztonsági funkciókhoz (amelyek hardverben, szoftverben vagy förmverben valósulnak meg) és információkhoz való hozzáférés az erre feljogosított személyzetre (pl. biztonsági adminisztrátorok) korlátozódjon.

HE-4 Információ áramlás ellenőrzés érvényre juttatása
Az informatikai rendszer a megfelelő szabályzattal összhangban érvényre juttatja a kiosztott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információ áramlás ellenőrzéséhez.

HE-5 A felelősségek szétválasztása
Az informatikai rendszer érvényre juttatja a felelősségek szétválasztását az egyes szerepkörökhöz kijelölt hozzáférési jogosultságokon keresztül.

HE-6 Legkisebb jogosultság
Az informatikai rendszer a felhasználók (illetve a felhasználók nevében fellépő eljárások) számára a megadott feladatok végrehajtásához szükséges leginkább korlátozó jogosultságok/privilégiumok, illetve hozzáférések összességét juttatják érvényre.

HE-7 Sikertelen bejelentkezési kísérletek
Az informatikai rendszer egy [*3*]-nak megadott korlátot juttat érvényre egy felhasználó egymást követő sikertelen bejelentkezési kísérleteire. Amennyiben a sikertelen kísérletek a megadott számot túllépik, az információs rendszer automatikusan [*zárolja a felhasználói fiókot*].

HE-8 A rendszerhasználat jelzése
Az informatikai rendszer egy jóváhagyott, a rendszerhasználatra vonatkozó jelzést ad a rendszerhez való hozzáférés engedélyezése előtt abból a célból, hogy a potenciális felhasználókat tájékoztatassa arról:

- hogy a felhasználó egy magyar közigazgatási informatikai rendszert használ;
- hogy lehetséges, hogy a rendszer használatot figyelhetik, rögzíthetik, illetve auditálhatják;
- hogy a rendszer jogosulatlan használata tilos, és büntetőjogi, valamint polgárjogi felelősségre vonással jár;
- hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. A rendszer által használt közlemény biztosítja a magántitokra és biztonságra vonatkozó értesítéseket, és mindaddig a képernyőn marad, amíg a felhasználó közvetlen műveletet nem végez az informatikai rendszerbe való bejelentkezéshez.

Megjegyzés: Mivel a DBCS rendszer egyetlen munkaállomásból áll, melyet összesen három személy működtet, ezért nincs szükség a potenciális felhasználók programozott tájékoztatására. A fenti figyelmeztetések üzemeltetési útmutatóba foglalásával a HE-8 követelmény teljesítettnek tekinthető.

HE-11 A munkaszakasz zárolása
Az informatikai rendszer [*30 perc*] inaktivitás után a munkaszakasz zárolásával megakadályozza a rendszerhez való további hozzáférést mindaddig, amíg a felhasználó nem azonosítja és hitelesíti magát újra a megfelelő eljárások alkalmazásával.

HE-12 A munkaszakasz lezárása
Az informatikai rendszer automatikusan lezárja a távoli munkaszakaszt egy, [értékadás: a szervezet által definiált időtartam] hosszúságú inaktivitás után.

Megjegyzés: Mivel a DBCS rendszer nem enged távoli hozzáférést, így nincs távoli munkaszakasz sem, következésképp a HE-8 követelmény teljesítettnek tekinthető.

HE-13 Felügyelet és felülvizsgálat — hozzáférés ellenőrzés
A szervezet felügyeli és felülvizsgálja a felhasználók tevékenységét az informatikai rendszer hozzáférés ellenőrzése érvényre juttatása és használata tekintetében.
(a) bővítés: A szervezet automatikus mechanizmusokat használ a felhasználói tevékenységek ellenőrzésére.

HE-14 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek
A szervezet meghatározza azokat a speciális felhasználói tevékenységeket, amelyeket az informatikai rendszerben azonosítás és hitelesítés nélkül is végre lehet hajtani.
(a) bővítés: A szervezet csak olyan mértékben engedélyezi az azonosítás és hitelesítés nélkül végrehajtható tevékenységeket, amennyire az saját céljainak megfelel.

HE-17 Távoli hozzáférés ellenőrzése
A szervezet engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való távoli hozzáférés minden módszerét (pl. betárcsázás, Internet), beleértve a privilegizált funkciókhoz való távoli hozzáférést. Megfelelően feljogosított tisztviselők engedélyezik az informatikai rendszerhez való hozzáférés minden egyes hozzáférési módszerét, és minden egyes hozzáférési módszer használatához csak a szükséges felhasználókat jogosítják fel.
(a) bővítés: A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módszerek figyelésére és ellenőrzésére.
(b) bővítés: A szervezet rejtjelzést alkalmaz a távoli hozzáférési munkaszakaszok bizalmasságának megvédésére.
(c) bővítés: A szervezet egy menedzselt hozzáférés ellenőrzési ponton keresztül minden távoli hozzáférést ellenőriz.
(d) bővítés: A szervezet magas jogosultsághoz kötött funkciókhoz csak komoly működéshez kapcsolódó igény esetén enged távoli hozzáférést, és ebben az esetben is dokumentálni kell ennek az indoklását az informatikai rendszer biztonsági tervében.

Megjegyzés: A DBCS rendszer nem tesz lehetővé távoli hozzáférést, következésképp a HE-17 követelmény és bővítései automatikusan teljesítettnek tekinthető.

HE-18 A vezeték nélküli hozzáférésre vonatkozó korlátozások
A szervezet:
- felhasználási korlátozásokat és megvalósítási útmutatót vezet be a vezeték nélküli technológiákra; és
- engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való vezeték nélküli hozzáféréseket.

(a) bővítés: A szervezet az informatikai rendszerhez való vezeték nélküli hozzáférés védelmére hitelesítést és rejtjelzést alkalmaz.

Megjegyzés: A DBCS rendszer nem tesz lehetővé vezeték nélküli hozzáférést, következésképp a HE-18 követelmény és bővítése automatikusan teljesítettnek tekinthető.

HE-19 A hordozható és mobil eszközök hozzáférés ellenőrzése
A szervezet:

- felhasználási korlátozásokat és megvalósítási útmutatót vezet be a hordozható és mobil eszközökre; és
- engedélyezi, figyeli és ellenőrzi az informatikai rendszerhez való, hordozható és mobil eszközökön keresztüli hozzáféréseket.
- Megfelelően feljogosított tisztviselők engedélyezik a hordozható és mobil eszközök használatát.

Megjegyzés: A DBCS rendszer nem teszi lehetővé hordozható és mobil eszközök használatát, következésképp a HE-19 követelmény automatikusan teljesítettnek tekinthető.

HE-20 Külső informatikai rendszerek használata
A szervezet meghatározza a feltételeket és szabályokat a feljogosított felhasználóknak a következőkre:

- hozzáférés az informatikai rendszerhez egy külső rendszerből;
- szervezet által ellenőrzött információk feldolgozása, tárolása és/vagy átvitele külső informatikai rendszerek segítségével.

(a) bővítés: A szervezet megtiltja a jogosult felhasználóknak külső informatikai rendszerek felhasználását a belső rendszeren található információk feldolgozására, tárolására vagy átvitelére, kivéve, ha a szervezet:

- ellenőrizni tudja a szükséges biztonsági intézkedések használatát a külső rendszeren, úgy ahogy az a biztonsági szabályzatban és biztonsági tervben le van írva;
- jóváhagyott kapcsolat van az informatikai rendszerek közt, vagy megállapodás született azzal a szervezettel, amelyik a külső informatikai rendszert befogadja.

Megjegyzés: A DBCS rendszer nem tesz lehetővé külső rendszerből történő hozzáférést, következésképp a HE-20 követelmény és bővítése automatikusan teljesítettnek tekinthető.

1.5.1.3 Rendszer és kommunikáció védelem (RV)

RV-1 Rendszer és kommunikáció védelmi szabályzat és eljárásrend
A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált, rendszer és kommunikáció védelmi szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettség, koordináció a szervezet egységei között, megfelelés, illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és kommunikáció védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RV-2 Alkalmazás szétválasztás
Az informatikai rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az informatikai rendszer menedzsment funkcionalitásától.

RV-4 Információ maradványok
Az informatikai rendszer meggátolja a megosztott rendszer erőforrások útján történő jogosulatlan és véletlen információáramlást.

RV-5 Szolgáltatás megtagadás elleni védelem
Az informatikai rendszer védelmet nyújt a következő típusú szolgáltatás megtagadás jellegű támadásokkal szemben vagy korlátozza azok kihatásait: [*valamennyi hálózat felöl induló, szolgáltatás megtagadásra irányuló támadás*].

Megjegyzés: A DBCS rendszer nem tesz lehetővé hálózati hozzáférést, következésképp az RV-5 követelmény automatikusan teljesítettnek tekinthető.

RV-7 A határok védelme
Az informatikai rendszer figyeli és ellenőrzi az informatikai rendszer külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációkat.
(a) bővítés: A szervezet a nyilvánosan hozzáférhető informatikai rendszer összetevőket (pl. nyilvános web szervereket) elkülönített alhálózatokban helyezi el, elkülönített fizikai hálózati interfészekkel. /Megjegyzés: Nyilvánosan hozzáférhető informatikai rendszer összetevő lehet például a web szerver. /
(b) bővítés: A szervezet meggátolja a nyilvános hozzáférést a szervezet belső hálózatához, kivéve azon eseteket, amikor a hozzáférés megfelelő védelmi intézkedések közbeiktatásával történik.
(c) bővítés: A szervezet korlátozza a hozzáférési pontok számát az informatikai rendszerhez, hogy jobban monitorozható legyen a kijövő és bejövő hálózati forgalom.
(d) bővítés: A szervezet kialakít egy felügyelt kapcsolódási pontot (határvédelmi eszközöket egy hatékony biztonsági architektúrában) a külső telekommunikációs szolgáltatóval, létrehozva azokat az intézkedéseket, amelyek szükségesek az átvitt információ bizalmasságának és integritásának védelméhez.
(e) bővítés: Az informatikai rendszer alapból tilt és kivételként engedélyez csak minden hálózati forgalmat (vagyis minden tiltva, engedélyezés kivételes esetben).

Megjegyzés: A DBCS rendszerben nincsenek nyilvánosan hozzáférhető informatikai rendszer összetevők, továbbá a rendszer nem tesz lehetővé se nyilvános hozzáférést, se kijövő és bejövő hálózati forgalmat, következésképp az RV-7 követelmény (a) - (e) bővítései automatikusan teljesítettnek tekinthetők.

RV-8 Az adatátvitel sértetlensége
Az informatikai rendszer megvédi a továbbított információk sértetlenségét.

RV-9 Az adatátvitel bizalmassága
Az informatikai rendszer megvédi az átvitt információk bizalmasságát.

RV-10 A hálózati kapcsolat megszakítása
Az informatikai rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, vagy [értékadás: a szervezet által meghatározott időtartam] hosszú inaktivitás után.

Megjegyzés: A DBCS rendszer nem tesz lehetővé hálózati kapcsolatot, következésképp az RV-10 követelmény automatikusan teljesítettnek tekinthető.

RV-12 Kriptográfiai kulcs előállítása és kezelése
Az informatikai rendszer a kriptográfiai kulcsok előállítására és kezelésére automatikus támogató eljárásokkal ellátott mechanizmusokat, vagy manuális eljárásokat alkalmaz.

RV-13 Jóváhagyott kriptográfia alkalmazása
Ha az informatikai rendszerben kriptográfiát alkalmaznak, a rendszer minden kriptográfiai műveletét (beleértve a kulcs előállítását is) szabványos algoritmussal kell megvalósítani.

RV-14 Sértetlenség védelem nyilvános hozzáférés esetén
A nyilvánosan elérhető rendszerek esetén az informatikai rendszer megvédi az információk és az alkalmazások sértetlenségét.

Megjegyzés: A DBCS rendszer nem elérhető nyilvánosan, következésképp az RV-14 követelmény automatikusan teljesítettnek tekinthető.

RV-15 Telekommunikációs szolgáltatások korlátozása
Az informatikai rendszer meggátolja a telekommunikációs szolgáltatások együttműködő számítógép-használati mechanizmusainak (pl. video és audio konferenciák) távolról történő aktiválását, és közvetlen jelzéseket biztosít az ilyen mechanizmusok használatról a lokális felhasználók felé (pl. kamera vagy mikrofon használata).

Megjegyzés: A DBCS rendszer nem elérhető távolról, következésképp az RV-15 követelmény automatikusan teljesítettnek tekinthető.

RV-17 Nyilvános kulcsú infrastruktúra tanúsítványok
Megfelelő hitelesítési rend szerint a szervezet vagy önmaga kiállít nyílt kulcsú tanúsítványt, vagy vásárol nyílt kulcsú tanúsítványt egy hitelesítés-szolgáltatótól.

Megjegyzés: A DBCS rendszer nem elérhető távolról, következésképp az RV-17 követelmény felesleges, ezért teljesítettnek tekinthető.

RV-18 Mobil kód korlátozása
A szervezet
- korlátozza a mobil kód technika alkalmazhatóságát, erre vonatkozó útmutatót bocsát ki, a mobil kódok rosszindulatú használata által okozott potenciális károk miatt, valamint
- dokumentálja, figyeli és ellenőrzi a mobil kódok információs rendszeren belüli felhasználását. Megfelelő vezető engedélyezi a mobil kódok használatát.

Megjegyzés: A DBCS rendszer nem alkalmaz mobil kód technikát, következésképp az RV-18 követelmény automatikusan teljesítettnek tekinthető.

RV-19 Interneten Keresztüli Hangátvitel (VoIP)
A szervezet:
- használati korlátozásokat vezet be és megvalósítási útmutatót ad az Interneten Keresztüli Hangátvitel (VoIP) technológiákhoz, a rosszindulatú használat esetén okozható károkat felmérve; és
- engedélyezi, figyeli, és ellenőrzi a VoIP használatát az informatikai rendszeren belül.

Megjegyzés: A DBCS rendszer nem alkalmaz VoIP technikát, következésképp az RV-19 követelmény automatikusan teljesítettnek tekinthető.

RV-20 Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)
Egy olyan informatikai rendszernek, amely az egész szervezet név/cím feloldó szolgáltatását biztosítja, a hiteles adatokon kívül egyéb biztonsági adatokat is vissza kell adnia a feloldási kérésekre, mint például az információ eredete és integritási adatok.

Megjegyzés: A DBCS rendszer nem biztosít név/cím feloldó szolgáltatást, következésképp az RV-20 követelmény automatikusan teljesítettnek tekinthető.

RV-22 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén
Egy olyan informatikai rendszernek, amely az egész szervezet név/cím feloldását szolgálja ki hibatűrőnek kell lennie, és működnie kell rajta a szerep szétválasztásnak.

Megjegyzés: A DBCS rendszer nem biztosít név/cím feloldó szolgáltatást, következésképp az RV-22 követelmény automatikusan teljesítettnek tekinthető.

RV-23 Munkaszakasz hitelessége
Az informatikai rendszer valamilyen mechanizmussal biztosítja a munkaszakaszok hitelességének védelmét.

1.5.1.4 Rendszer és információ sértetlenség (RS)

RS-1 Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend
A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált, rendszer és információ sértetlenségre vonatkozó szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettség, koordináció a szervezet egységei között, megfelelés, illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a rendszer és információ sértetlenségére vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

RS-2 Hibajavítás
A szervezet az informatikai rendszerben talált hibákat jelenti, és kijavítja.
(b) bővítés: A szervezet rendszeres időszakonként vagy szükség esetén automatikus mechanizmusokat alkalmaz az informatikai rendszer hibajavítási állapotának meghatározására.

RS-3 Rosszindulatú kódok elleni védelem
Az informatikai rendszer rosszindulatú kódok elleni védelmet valósít meg, s ez automatikus frissítési lehetőséget is magában foglal.
(a) bővítés: A szervezet központilag kezeli a vírusvédelmi mechanizmusokat.
(b) bővítés: Az informatikai rendszer automatikusan frissíti a rosszindulatú kódok elleni védelmi mechanizmust.
Megjegyzés: Mivel a DBCS rendszer egyetlen, hálózatra nem kapcsolódó munkaállomásból áll, se szükség, se lehetőség nincs központi kezelésre, automatikus frissítési lehetőségre. Következésképp az RS-3 követelmény második fele (automatikus frissítési lehetőség), valamint a követelmény bővítései automatikusan teljesítettnek tekinthetők.

RS-4 Behatolás észlelési eszközök és technikák
A szervezet eszközöket és technikákat alkalmaz az informatikai rendszerben történő események figyelésére, detektálja a támadásokat, és biztosítja a rendszer jogosulatlan használatának beazonosítását.
(d) bővítés: Az informatikai rendszer monitorozza a kimenő és bejövő kommunikációt, keresve a szokatlan és nem engedélyezett tevékenységeket és feltételeket. /Magyarázat: Szokatlan/nem engedélyezett tevékenységek vagy feltételek közé tartozhat például a rosszindulatú kód jelenléte, az információ nem engedélyezett exportálása, vagy külső informatikai rendszer felé történő jelzés küldése./

Megjegyzés: A DBCS rendszer nem tesz lehetővé hálózati kapcsolatot, következésképp az RS-4 követelmény és bővítése automatikusan teljesítettnek tekinthető.

RS-5 Biztonsági riasztások és tájékoztatások
A szervezet folyamatosan fogadja az informatikai rendszerre vonatkozó biztonsági riasztásokat és figyelmeztetéseket, eljuttatja ezeket az illetékes személyekhez, illetve megfelelő válaszlépéseket foganatosít.

Megjegyzés: A DBCS rendszer nem tesz lehetővé hálózati kapcsolatot, következésképp az RS-5 követelmény automatikusan teljesítettnek tekinthető.

RS-8 Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem
Az informatikai rendszer kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelmet valósít meg.

Megjegyzés: A DBCS rendszer off-line, nem teszi lehetővé levelek fogadását, következésképp az RS-8 követelmény automatikusan teljesítettnek tekinthető.

RS-9 A bemeneti információra vonatkozó korlátozások
A szervezet az informatikai rendszernek szóló információ bevitelt az erre jogosult személyekre korlátozza.

RS-10 A bemeneti információ pontossága, teljessége, érvényessége és hitelessége
Az informatikai rendszer ellenőrzi az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét.

RS-11 Hibakezelés
Az informatikai rendszer eredményesen azonosítja és kezeli a hibákat, de nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak.

RS-12 A kimeneti információ kezelése és megőrzése
A szervezet az informatikai rendszer kimenetét a szervezeti szabályzattal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

1.5.1.5 Naplózás és elszámoltathatóság (NA)

NA-1 Naplózási és elszámoltathatósági szabályzat és eljárásrend
A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált naplózási szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettség, koordináció a szervezet egységei között, megfelelés, illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a naplózási szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

NA-2 Naplózandó események
Az informatikai rendszer naplóbejegyzéseket állít elő a következő eseményekre: [*a naplózási és elszámoltathatósági szabályzatban meghatározott naplózandó események*].
(c) bővítés: A szervezet időnként felülvizsgálja és frissíti a szervezet által naplózandó események listáját.

NA-3 A naplóbejegyzések tartalma
Az informatikai rendszer a naplóbejegyzésekben elegendő információt gyűjt be ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.
(a) bővítés: Az informatikai rendszer lehetőséget nyújt arra, hogy a fentieken túl, részletesebb információkat is be lehessen venni, a naplóbejegyzések típusa, elhelyezkedése vagy tárgya alapján.

Megjegyzés: A DBCS rendszerben összesen két célszoftver fut (rgen és dbcs), melynek naplózása az előre látható igények alapján került megtervezésre. Várhatóan nem lesz szükség a naplózandó események későbbi bővítésére. Amennyiben mégis részletesebb naplóinformációra lenne szükség, a célszoftverek módosításával (részletesebb naplózási funkció beépítésével) ezt is meg lehet oldani a jövőben. Ezzel a megjegyzéssel az NA-3 (a) bővítésében szereplő követelmény automatikusan teljesítettnek tekinthető.

NA-4 Napló tárkapacitás
A szervezet a naplózásra elegendő méretű tárkapacitást jelöl ki, illetve úgy konfigurálja a naplózást, hogy megelőzze az adott tárkapacitás betelését.

NA-5 Naplózási hiba kezelése
Naplózási hiba esetén, vagy ha a naplózás tárkapacitás beteléshez közelít, az informatikai rendszer riasztást küld az adminisztrátornak, valamint a következő tevékenységeket is elvégzi: [*az informatikai rendszer leállítása*].

Megjegyzés: A DBCS rendszerben minden adatbázis összekapcsolási projekt esetében a keletkezett naplóállományokat adathordozóra másolják, mielőtt a teljes rendszert törölnék. Egy új adatbázis összekapcsolási projekt mindig az eredeti mesterpéldányból indul. Ebben olyan nagy mennyiségű tárhely biztosított, hogy az eredményeknek és a naplóállományoknak mindig biztosan marad hely. Következésképpen az NA-5 követelményt csak a (hardver vagy szoftver hibából adódó) naplózási hibára kell kielégíteni, a naplózás tárkapacitására vonatkozó részek automatikusan teljesítettnek tekinthetők.

NA-6 Napló figyelése, vizsgálata és jelentések készítése
A szervezet rendszeresen áttekinti/átvizsgálja a naplóbejegyzéseket, nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, elemzi a gyanús tevékenységeket és a feltételezett megsértéseket, jelenti ezeket a megfelelő tisztviselőknek, illetve megteszi a szükséges intézkedéseket.
(b) bővítés: A szervezet automatikus mechanizmusokat használ a biztonsági személyzet riasztására a következő gyanús vagy szokatlan események esetén: [értékadás: a szervezet által meghatározott lista a gyanús vagy szokatlan eseményekről, amelyek esetén riasztás szükséges].

Megjegyzés: A rendszervizsgálónak adathordozón átadott naplóbejegyzések áttekintése és átvizsgálása a DBCS rendszeren kívül történik, így az NA-6 követelmény nem vonatkozik a DBCS rendszerre, ezért (a DBCS rendszeren belül) automatikusan teljesítettnek tekinthető.

Megjegyzés: A DBCS rendszer egy olyan off-line rendszer, mely csak időszakosan működik, akkor is mindig a rendszervizsgáló személyes felügyelete alatt. Következésképp minden gyanús esemény a rendszervizsgáló tudomására jut, ezért nincs szükség automatikus riasztási mechanizmusok használatára, az NA-6 követelmény (b) bővítése teljesítettnek tekinthető.

NA-7 Naplócsökkentés, naplóriport készítés
Az informatikai rendszer lehetőséget biztosít naplócsökkentésre és naplóriport készítésére.
(a) bővítés: Az informatikai rendszer biztosítja, hogy automatikusan fel lehessen dolgozni az érdekes naplóbejegyzéseket egy kiválasztható, feltétel alapú rendszer alapján.

Megjegyzés: A naplóbejegyzések feldolgozása a DBCS rendszeren kívül történik, így az NA-7 követelmény és annak (a) bővítése nem vonatkoznak a DBCS rendszerre, ezért (a DBCS rendszeren belül) automatikusan teljesítettnek tekinthetők.

NA-8 Időbélyegek
Az informatikai rendszer időbélyegeket biztosít a naplóbejegyzések előállításához.
(a) bővítés: A szervezet szinkronizálja a belső rendszer órákat a következő gyakorisággal [*minden egyes adatkérést kiszolgáló tevékenységénél*].

NA-9 A napló információk védelme
Az informatikai rendszer megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

NA-11 A naplóbejegyzések megőrzése
A szervezet a naplóbejegyzéseket megőrzi [*5 évig*]-ig abból a célból, hogy támogatást nyújtson a rendkívüli események utólagos kivizsgálására, és hogy megfeleljen a jogszabályi és szervezeti információ megőrzési követelményeknek.

1.5.1.6 Konfiguráció kezelés (KK)

KK-1 Konfiguráció kezelési szabályzat és eljárásrend
A szervezet kifejleszt, terjeszt és rendszeresen felülvizsgál/frissít:

- egy formális, dokumentált konfiguráció kezelési szabályzatot, amely az alábbi témaköröket tárgyalja: célok, hatókör, szerepkörök, felelősségek, vezetői elkötelezettség, koordináció a szervezet egységei között, megfelelés, illetve
- egy formális, dokumentált eljárásrendet, amelynek célja a konfiguráció kezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósításának elősegítése.

KK-2 Alap konfiguráció
A szervezet informatikai célrendszeréhez egy alap konfigurációt fejleszt ki, dokumentálja és karbantartja a rendszer lényeges komponenseit.
(a) bővítés: A szervezet az alap konfiguráció frissítését az informatikai rendszer komponensek telepítésének a szerves részeként végzi.

KK-3 A konfigurációváltozások ellenőrzése
A szervezet dokumentálja és ellenőrzi az informatikai rendszerben történt változásokat. Megfelelő szervezeti tisztviselők hagyják jóvá az informatikai rendszer változásait, összhangban a szervezeti szabályzatokkal és eljárásrendekkel.

KK-4 A konfigurációváltozások felügyelete
A szervezet figyeli az informatikai rendszerben történt változásokat, és biztonsági hatásvizsgálatot végez a változások hatásainak meghatározására.

KK-5 A változtatásokra vonatkozó hozzáférés korlátozások
A szervezet hozzáférési korlátozásokat juttat érvényre az informatikai rendszer (konfigurációs) változtatásaival kapcsolatban.

KK-6 Konfigurációs beállítások
A szervezet

- kötelező konfigurációs beállítást határoz meg az informatikai rendszerben használt információ technológiai termékekre;
- az információ technológiai termékek lehető legkorlátozóbb biztonsági beállításait konfigurálja, amely még megfelel a működési követelményeknek;
- dokumentálja a konfigurációs beállításokat; és
- érvényre juttatja a konfigurációs beállításokat az informatikai rendszer valamennyi komponensében.

KK-7 Legszűkebb funkcionalitás
A szervezet az informatikai rendszert úgy konfigurálja, hogy az csak a szükséges lehetőségeket nyújtsa, illetve letiltja/korlátozza a következő funkciók, portok, protokollok és/vagy szolgáltatások használatát: *[hálózatra kapcsolódás]*.

KK-8 Informatikai rendszer komponens leltár
A szervezet aktuális leltárt készít, dokumentálja és karbantartja az informatikai rendszer komponenseit és a vonatkozó tulajdonosi információkat.
(a) bővítés: A szervezet az informatikai rendszer komponensek leltárjának a frissítését a komponensek telepítésének a szerves részeként végzi.

1.5.1.7 Speciális kiegészítő elvárások (SK)

A fokozott kihatású biztonsági osztály fentiekben meghatározott általános követelményei között nem szerepel néhány olyan elvárás, melyet az [1] és [2] jogszabályok elvárnak.

Az alábbi kiegészítő követelmények ezen jogszabályi elvárásokat fedik le.

SK-1 Adatbázis elemek összekapcsolása

A rendszernek képesnek kell lennie különböző adatkezelők adatbázisaiból származó adatok összekapcsolására, az alábbi feltételekkel:

- a különböző adatkezelők adatbázisaiból az azonos alanyra vonatkozó adatelemeket kell összekapcsolni,
- az összekapcsolás alapja egy olyan személyazonosító adat (adóazonosító jel, társadalombiztosítási azonosító jel, személyazonosító jel, vagy név és lakcím együttese) legyen, melynek kezelésére valamennyi adatkezelő jogosult,
- az összekapcsolás konkrét megvalósítása az alapját képező személyazonosító adatra (egy azonos kódképzési módszer alapján) számolt anonim kapcsolati kóddal történjen.

SK-2 Minősített hash függvény

Az anonim kapcsolati kódképzés kriptográfiailag erős legyen, hogy megszüntesse a személyességet, alkalmazásával visszafordíthatatlanul elvesszen az alanyával való kapcsolata, az összekapcsolt adatokból ne lehessen visszakövetkeztetni az adatok alanyára.
A rendszernek olyan hash-függvényt kell előállítania és adathordozóra másolnia, melyre igazoltan teljesülnek az alábbi tulajdonságok:

- egyirányúság (one-way function),
- szigorú lavina-hatás (strict avalanche criterion),
- ütközés-ellenállóság (collisison resistance),
- hossznövekedés elleni támadások elleni ellenállás (resistance to lenght-extensions attacks),
- „véletlenszerű” leképezésként való viselkedés (random oracle model),
- nehezen invertálhatóság rövid bemenő adatra,
- a bemenetek teljes kipróbálásának kizárása rövid bemenő adatra.

SK-3 Véletlenített hash függvény

Az anonim kapcsolati kódképzés konkrét módszerének egyedi, véletlenszerűen megállapított elemeket is tartalmaznia kell.
A rendszernek a hash-függvény paraméterezéséhez olyan véletlen elemeket kell generálnia és adathordozóra másolnia, melyekre teljesülnek az alábbi tulajdonságok:

- a véletlen generálás elvi megfelelősége,
- legalább 100 bit szabadságfok biztosítása.

SK-4 Visszaállíthatatlan törlés

Az összekapcsolás után a kapcsolati kódokat és a kapcsolás módszerét is törölni kell.
A rendszernek biztosítania kell, hogy egy erőforrás korábbi információtartalma hozzáférhetetlenné válik az erőforrás használat utáni közvetlen deallokációja után az alábbi objektumokra:

- a hash-függvény paraméterezéséhez generált véletlen elemek,
- a kapcsolati kódok (az összekapcsolást megalapozó hash értékek).

1.5.2 A biztonsági követelmények indoklása

A 6. táblázat az előző alfejezetben meghatározott követelményeket visszavezeti a DBCS rendszer biztonsági céljaira.

a DBCS rendszerre vonatkozó biztonsági követelmény	a DBCS rendszerre vonatkozó biztonsági cél
SK-1 (Adatbázis elemek összekapcsolása)	O1 (Az összekapcsolt adatok alanyának védelme)
SK-2 (Minősített hash függvény)	O1
SK-3 (Véletlenített hash függvény)	O2 (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása)
SK-4 (Visszaállíthatatlan törlés)	O2
AH (Azonosítás és hitelesítés)	O1, O2
HE (Hozzáférés ellenőrzése)	O1, O2
RV (Rendszer és kommunikáció védelem)	O1, O2
RS (Rendszer és információ sértetlenség)	O1, O2
NA (Naplózásra és elszámoltathatóság)	O1, O2
KK (Konfiguráció kezelés)	O1, O2

6. táblázat: A biztonsági követelmények és a biztonsági célok közötti megfeleltetés

A 6. táblázatból látható, hogy minden biztonsági követelmény teljesítés hozzájárul legalább egy biztonsági cél teljesüléséhez.

Az **O1 biztonsági cél** (Az összekapcsolt adatok alanyának védelme) teljesüléséhez közvetlenül hozzájárul:

- **SK-1** (Adatbázis elemek összekapcsolása) azáltal, hogy az összekapcsolás konkrét megvalósítása nem az alapját képező személyazonosító adatra, hanem egy (azonos kódképzési módszer alapján számolt) anonim kapcsolati kóddal történik.
- **SK-2** (Minősített hash függvény) azáltal, hogy az anonim kapcsolati kódképzés kriptográfiailag erős, így megszünteti a személyességet, alkalmazásával visszafordíthatatlanul elveszik az alanyával való kapcsolata, s az összekapcsolt adatokból nem lehet visszakövetkeztetni az adatok alanyára.

Az **O1 biztonsági cél** teljesülését közvetve támogatja:

- **AH** (Azonosítás és hitelesítés) azáltal, hogy egyedileg és biztonságos módon azonosítja és hitelesíti a felhasználókat, megteremti a hozzáférés ellenőrzés (HE) és az elszámoltathatóság (NA) alapját.
- **HE** (Hozzáférés ellenőrzése) azáltal, hogy a rendszerben különböző szerepköröket betöltő felhasználók csak a számukra kijelölt, szétválasztott és minimalizált hozzáférési jogosultságokon keresztül aktivizálhatják a rendszert, így nem sérthetik meg a biztonságos működtetés szabályait, nem kerülhetik meg az SK-1 és SK-2 követelmények teljesítését.
- **RV** (Rendszer és kommunikáció védelem) azáltal, hogy biztosítja a rendszer helyes működését, megakadályozza a jogosulatlan és véletlen információáramlást, megvédi a továbbított információk sértetlenségét és bizalmasságát, támogatja az SK-1 és SK-2 követelmények teljesítését.

- **RS** (Rendszer és információ sértetlenség) azáltal, hogy rosszindulatú kódok elleni védelmet valósít meg, az információ bevitelt az erre jogosult személyekre korlátozza, ellenőrzi az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét, biztonságos módon azonosítja és kezeli a hibákat, támogatja az SK-1 és SK-2 követelmények teljesítését.
- **NA** (Naplózás és elszámoltathatóság) azáltal, hogy a naplóbejegyzésekben elegendő információt gyűjt be annak kimutatásához, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele, megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben, támogatást nyújt a rendkívüli események utólagos kivizsgálására, hozzájárul a rendszer helyes működtetéséhez, támogatja az SK-1 és SK-2 követelmények teljesítését.
- **KK** (Konfiguráció kezelés) azáltal, hogy dokumentálja és karbantartja az informatikai célrendszer alap konfigurációját, dokumentálja és ellenőrzi az informatikai rendszerben történt változásokat, biztonsági hatásvizsgálatot végez a változások hatásainak meghatározására, hozzáférési korlátozásokat juttat érvényre az informatikai rendszer konfigurációs változtatásaival kapcsolatban, letiltja a rendszer hálózatra kapcsolódását, hozzájárul a rendszer helyes működéséhez, s ezzel támogatja az SK-1 és SK-2 követelmények teljesítését.

Az **O2 biztonsági cél** (Különböző összekapcsolások ismételt összekapcsolásának megakadályozása) teljesüléséhez közvetlenül hozzájárul:

- **SK-3** (Véletlenített hash függvény) azáltal, hogy az anonim kapcsolati kód képzési módszerében véletlenszerű elemeket is használ, s így több adatkérést nem lehet ugyanazzal a kóddal megvalósítani, ezáltal ezek eredményeit még az adatkérő és az adatkezelő sem képes összevonni.
- **SK-4** (Visszaállíthatatlan törlés) azáltal, hogy az anonim kapcsolati kódot generálás és átadás után haladéktalanul törli, még az adatbázis létrehozásáért felelős szerv sem képes különböző összekapcsolások eredményeit utólag összevonni.

Az **O2 biztonsági cél** teljesülését közvetve támogatja:

- **AH** (Azonosítás és hitelesítés) azáltal, hogy egyedileg és biztonságos módon azonosítja és hitelesíti a felhasználókat, megteremti a hozzáférés ellenőrzés (HE) és az elszámoltathatóság (NA) alapját.
- **HE** (Hozzáférés ellenőrzése) azáltal, hogy a rendszerben különböző szerepköröket betöltő felhasználók csak a számukra kijelölt, szétválasztott és minimalizált hozzáférési jogosultságokon keresztül aktivizálhatják a rendszert, így nem sérthetik meg a biztonságos működtetés szabályait, nem kerülhetik meg az SK-3 és SK-4 követelmények teljesítését.
- **RV** (Rendszer és kommunikáció védelem) azáltal, hogy biztosítja a rendszer helyes működését, megakadályozza a jogosulatlan és véletlen információáramlást, megvédi a továbbított információk sértetlenségét és bizalmasságát, támogatja az SK-3 és SK-4 követelmények teljesítését.
- **RS** (Rendszer és információ sértetlenség) azáltal, hogy rosszindulatú kódok elleni védelmet valósít meg, az információ bevitelt az erre jogosult személyekre korlátozza, ellenőrzi az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét, biztonságos módon azonosítja és kezeli a hibákat, támogatja az SK-3 és SK-4 követelmények teljesítését.

- **NA** (Naplózás és elszámoltathatóság) azáltal, hogy a naplóbejegyzésekben elegendő információt gyűjt be annak kimutatásához, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele, megvédi a napló információt és a naplózás eszközeit a jogosulatlan hozzáféréssel, módosítással és törléssel szemben, támogatást nyújt a rendkívüli események utólagos kivizsgálására, hozzájárul a rendszer helyes működtetéséhez, támogatja az SK-1 és SK-2 követelmények teljesítését.
- **KK** (Konfiguráció kezelés) azáltal, hogy dokumentálja és karbantartja az informatikai célrendszer alap konfigurációját, dokumentálja és ellenőrzi az informatikai rendszerben történt változásokat, biztonsági hatásvizsgálatot végez a változások hatásainak meghatározására, hozzáférési korlátozásokat juttat érvényre az informatikai rendszer konfigurációs változtatásaival kapcsolatban, letiltja a rendszer hálózatra kapcsolódását, hozzájárul a rendszer helyes működéséhez, s ezzel támogatja az SK-3 és SK-4 követelmények teljesítését.

1.5.3 A rendszerre elvárt garanciák

A rendszer egészére elvárt garancia a [7] által meghatározott fokozott szintű (SAP-F) garanciacsomag.

A 7. táblázat a SAP-F garancia-összetevőit tartalmazza:

Rendszer fejlesztés (ASDV)	ASDV_SIS.1	Informális interfész specifikáció
	ASDV_ARC.1	Biztonsági szerkezet leírás
	ASDV_SDS.1	Alrendszer és komponens szintű biztonsági terv
	ASDV_OSC.1	Rendszer-működési biztonsági koncepció
Rendszer útmutató dokumentumok (ASGD)	ASGD_PRE.2	Az előkészítési útmutató igazolása
	ASGD_CON.2	A konfigurálási útmutató igazolása
	ASGD_OPE.2	Az üzemeltetési útmutató igazolása
Rendszer konfiguráció kezelés (ASCM)	ASCM_SBC.2	A rendszer alap konfiguráció igazolása
	ASCM_ECC.2	A tanúsított komponensek ellenőrzése
Rendszer tesztelés (ASTE)	ASTE_FUN.1	Funkcionális tesztelés
	ASTE_COV.1	A teszt lefedettség vizsgálata
	ASTE_DPT.2	Tesztelés: alrendszerek
	ASTE_IND.1	Független tesztelés mintán
Rendszer sebezhetőség felmérés (ASVA)	ASVA_VAN.2	Független sebezhetőség vizsgálat

7. táblázat: A SAP-F garancia-összetevői

1.5.3.1 Informális interfész specifikáció (ASDV_SIS.1)

ASDV_SIS.1.1D A rendszer integrátornak biztosítania kell egy rendszer interfész specifikációt.

ASDV_SIS.1.1C A rendszer interfész specifikációnak informális stílusban le kell írnia az STOE biztonsági funkcionalitását (SSF) és annak külső interfészeit.

ASDV_SIS.1.2C A rendszer interfész specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ASDV_SIS.1.3C A rendszer interfész specifikációnak le kell írnia az SSF minden külső interfészére a használat célját és módját, részletezve a hatásokat, kivételeket és hibaüzeneteket.

ASDV_SIS.1.4C A rendszer interfész specifikációnak teljes mértékben be kell mutatnia az SSF-et.

ASDV_SIS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SIS.1.2E Az értékelőnek meg kell állapítania, hogy a rendszer interfész specifikáció az STOE funkcionális biztonsági követelményeinek pontos és teljes megjelenítése.

1.5.3.2 Biztonsági szerkezet leírás (ASDV_ARC.1)

ASDV_ARC.1.1D A rendszer integrátornak úgy kell megterveznie és megvalósítania az STOE-t, hogy a rendszer biztonsági funkcionalitását ne lehessen megkerülni.

ASDV_ARC.1.2D A rendszer integrátornak úgy kell megterveznie és megvalósítania a rendszer biztonsági funkcionalitását, hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

ASDV_ARC.1.3D A rendszer integrátornak biztosítania kell egy leírást az STOE biztonsági architektúrájáról.

ASDV_ARC.1.1C A biztonsági architektúra leírásnak ismertetnie kell az STOE-hez kapcsolódó külső informatikai rendszereket, egymáshoz kapcsolódásukat, valamint a köztük folyó információáramlást.

ASDV_ARC.1.2C A biztonsági architektúra leírásnak ismertetnie kell az STOE biztonsági funkcionalitás szerkezetét, olyan részletességgel, amely összemérhető a rendszer interfész specifikáció és az STOE terv részletességével.

ASDV_ARC.1.3C A biztonsági architektúra leírásnak szemléltetnie kell, hogy az STOE meggátolja a funkcionális biztonsági követelményeket érvényre juttató funkcionalitás megkerülését.

ASDV_ARC.1.4C A biztonsági architektúra leírásnak szemléltetnie kell, hogy a rendszer biztonsági funkcionalitás megvédi magát a hamisítással szemben.

ASDV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.5.3.3 Alrendszer és komponens szintű biztonsági terv (ASDV_SDS.1)

ASDV_SDS.1.1D A rendszer integrátornak biztosítania kell az STOE rendszer biztonsági tervét (STOE tervét).

ASDV_SDS.1.2D A rendszer integrátornak egy leképezést kell biztosítania a rendszer interfész specifikációban meghatározott rendszer biztonsági funkcionalitás interfész (SSFI) és az STOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

ASDV_SDS.1.1C Az STOE tervnek le kell írnia az STOE szerkezetét alrendszerek szerint.

ASDV_SDS.1.2C Az STOE tervnek azonosítania kell az SSF minden alrendszerét.

ASDV_SDS.1.3C Az STOE tervnek leírást kell biztosítania az SSF összes alrendszeréről.

ASDV_SDS.1.4C Az STOE tervnek le kell írnia az SSF összes alrendszere közötti kapcsolatokat.

ASDV_SDS.1.5C Az STOE tervnek le kell írnia az SSF-et komponensek szerint.

ASDV_SDS.1.6C Az STOE tervnek egy leképezést kell biztosítania az SSF alrendszerei és az SSF komponensei között.

ASDV_SDS.1.7C Az STOE tervnek le kell írnia az összes SFR-t érvényre juttató komponenst, megadva céljukat és a többi komponenssel való kapcsolatukat.

ASDV_SDS.1.8C Az STOE tervnek le kell írnia az összes SFR-t érvényre juttató komponenst, megadva az SFR vonatkozású interfészeiket, ezen interfészek visszatérési értékeit, valamint a többi komponenssel való kapcsolatukat és a meghívott interfészeket.

ASDV_SDS.1.9C Az STOE tervnek le kell írnia az összes SFR-t támogató, illetve az SFR-be nem beavatkozó komponenst, megadva céljukat és a többi komponenssel való kapcsolatukat.

ASDV_SDS.1.10C A leképezésnek szemléltetnie kell, hogy az STOE tervben leírt minden működést leképezi az ezeket meghívó SSFI-kre.

ASDV_SDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SDS.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE terv az összes funkcionális biztonsági követelmény pontos és teljes megjelenítése.

1.5.3.4 Rendszer-működési biztonsági koncepció (ASDV_OSC.1)

ASDV_OSC.1.1D A rendszer integrátornak biztosítania kell a rendszer-működésre vonatkozó biztonsági koncepció leírását.

ASDV_OSC.1.1C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer belső (rendszer határain belüli) információ áramlást érvényre juttató képességét.

ASDV_OSC.1.2C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer külső (külső rendszerek felé történő) információ áramlást érvényre juttató képességét.

ASDV_OSC1.3C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer lokális és távoli hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.4C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer erőforrásokhoz való (hozzáférés közvetítési szabályokon alapuló) hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.5C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer által nyújtott üzemmódokat, az üzemmódok közötti átmenetek feltételeit, és azokat az érvényesítő mechanizmusokat, amelyek minden azonosított rendszer üzemmódban biztonságos működést biztosítanak.

ASDV_OSC.1.6C A rendszer-működési biztonsági koncepció leírásának belső ellentmondástól mentesnek kell lennie.

ASDV_OSC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_OSC.1.2E Az értékelőnek meg kell állapítania a rendszer architektúra leírásról és az STOE tervről, hogy azok teljesen megvalósítják a rendszer-működési biztonsági koncepciót.

1.5.3.5 Az előkészítési útmutató igazolása (ASGD_PRE.2)

ASGD_PRE.2.1D A rendszer integrátornak a működőképes STOE mellé biztosítania kell az előkészítési útmutatót.

ASGD_PRE.2.1C Az előkészítési útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.2.2C Az előkészítési útmutatónak le kell írnia az STOE komponenseinek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

ASGD_PRE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_PRE.2.2E Az értékelőnek független ellenőrzést kell végeznie az előkészítési útmutató tartalmának gyakorlati alkalmazására vonatkozóan az alábbiak útján: [*személyi interjúk, az előkészítési útmutató mintavételezése, az előkészítés eredményének mintavételen alapuló független vizsgálata*].

1.5.3.6 A konfigurálási útmutató igazolása (ASGD_CON.2)

ASGD_CON.2.1D A rendszer integrátornak biztosítania kell egy konfigurálási útmutatót, amely meghatározza azokat a biztonság-vonzatú konfigurációs paramétereket, amelyek támogatják a rendszer komponenseinek az integrálását, és amelyek lehetővé teszik, hogy a szolgáltató rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a szolgáltató rendszer működésre vonatkozó biztonsági koncepcióját és a kapcsolódó szabályzatokat.

ASGD_CON.2.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.2.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.2.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.2.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.2.5C A konfigurálási útmutatónak ellentmondásmentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.2.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.2.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

ASGD_CON.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.5.3.7 Az üzemeltetési útmutató igazolása (ASGD_OPE.2)

ASGD_OPE.2.1D A rendszer integrátornak üzemeltetési útmutatót kell biztosítania.

ASGD_OPE.2.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

ASGD_OPE.2.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

ASGD_OPE.2.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

ASGD_OPE.2.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

ASGD_OPE.2.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemeltetési hiba utáni műveleteket is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

ASGD_OPE.2.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

ASGD_OPE.2.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

ASGD_OPE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_OPE.2.2E Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató specifikációinak gyakorlati alkalmazását illetően, az alábbiak útján: [*személyi interjúk, az üzemeltetési útmutató mintavételezése, az üzemeltetés eredményeinek mintavételen alapuló független vizsgálata*].

1.5.3.8 A rendszer alap konfiguráció igazolása (ASCM_SBC.2)

ASCM_SBC.2.1D A rendszer integrátornak konfiguráció kezelés (CM) rendszert kell használnia a legutolsó rendszer értékelés során értékelt rendszerhez, mely utóbbit „alap konfiguráció”-nak kell nevezni.

ASCM_SBC.2.2D A CM rendszernek nyomon kell követnie és felügyelnie kell minden tervezett és tényleges változtatást a rendszer alap konfigurációján, valamint ezek értékelési állapotát.

ASCM_SBC.2.3D A rendszer integrátornak vagy rendszertulajdonosnak CM dokumentációt kell nyújtania a rendszer alap konfigurációjához.

ASCM_SBC.2.1C A CM rendszernek egyedileg azonosítania kell az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.2.2C A CM rendszernek nyomon kell követnie az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.2.3C A CM dokumentációnak le kell írnia, hogy a rendszer alap konfigurációját hogyan kezelik, és hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik, és hogyan követik nyomon.

ASCM_SBC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_SBC.2.2E Az értékelőnek független ellenőrzést kell végeznie a CM rendszer alap konfiguráció tartalmára vonatkozóan, személyi interjúk és a módosítások mintavételezése útján.

1.5.3.9 A tanúsított komponensek ellenőrzése (ASCM_ECC.2)

ASCM_ECC.2.1D A rendszer integrátornak az STOE alap konfigurációját alkotó termék-komponensek közül meg kell határoznia az értékelt és tanúsított termék-komponensek listáját, valamint az ezekre vonatkozó garancia csomagokat.

ASCM_ECC.2.2D A rendszer integrátornak specifikálnia kell minden értékelt és tanúsított rendszer komponensre a termék üzemeltetési feltételeit.

ASCM_ECC.2.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garancia csomagjait.

ASCM_ECC.2.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.2.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia a tanúsítványban meghatározott, a biztonságos üzemeltetésre vonatkozó feltételeket.

ASCM_ECC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.2.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott, a biztonságos üzemeltetésre vonatkozó feltételeket.

ASCM_ECC.2.3E Az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek rendelkeznek legalább CC EAL2 vagy MIBÉTS alap szintű, a biztonsági funkcionalitást érvényre juttató komponensek pedig legalább CC EAL3 vagy MIBÉTS fokozott szintű tanúsítással.

1.5.3.10 Funkcionális tesztelés (ASTE_FUN.1)

ASTE_FUN.1.1D A rendszer integrátornak tesztelnie kell a rendszer biztonsági funkcionalitását (SSF-t), és ennek eredményeit dokumentálnia kell.

ASTE_FUN.1.2D A rendszer integrátornak tesztdokumentációt kell biztosítania.

ASTE_FUN.1.3D A rendszer integrátornak vizsgálatot kell biztosítania a tesztelése teljességéről.

ASTE_FUN.1.1C A tesztdokumentációnak tartalmaznia kell a teszttterveket, a várt teszteredményeket és a tényleges teszteredményeket.

ASTE_FUN.1.2C A teszttterveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ASTE_FUN.1.3C A várt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ASTE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk a várt teszteredményekkel.

ASTE_FUN.1.5C A tesztdokumentációnak vizsgálatot kell tartalmaznia a teszt eljárás sorrendi függőségeiről.

ASTE_FUN.1.6C A biztonsági intézkedések tesztelésének részletességére vonatkozó vizsgálatának be kell mutatnia, hogy az SST-ben elvárt funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

ASTE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.5.3.11 A teszt lefedettség vizsgálata (ASTE_COV.1)

ASTE_COV.1.1D A rendszer integrátornak biztosítania kell a teszt lefedettség elemzését.

ASTE_COV.1.1C A teszt lefedettség elemzésnek be kell mutatnia a tesztdokumentációban azonosított tesztek és a rendszer biztonsági funkcionalitás (ahogyan azt a rendszer interfész specifikáció a külső interfészeken keresztül leírja) közötti megfeleltetést.

ASTE_COV.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.5.3.12 Tesztelés: alrendszerek (ASTE_DPT.2)

ASTE_DPT.2.1D A rendszer integrátornak tesztmélység elemzést kell biztosítania.

ASTE _DPT.2.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással, valamint a rendszer biztonsági

ASTE_DPT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.5.3.13 Független tesztelés mintán (ASTE_IND.1)

ASTE_IND.1.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

ASTE_IND.1.1C Az STOE-nek tesztelésre alkalmas állapotban kell lennie.

ASTE_IND.1.2C A rendszer integrátornak biztosítania kell az SSF funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

ASTE_IND.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_IND.1.2E Az értékelőnek végre kell hajtania a tesztdokumentációban szereplő tesztek valamely részhalmazát (mintáját) a rendszer integrátor teszteredményeinek ellenőrzése érdekében.

ASTE_IND.1.3E Az értékelőnek tesztelnie kell az SSF külső és belső interfészeinek egy részét annak megerősítése érdekében, hogy az SSF a specifikáltaknak megfelelően működik.

1.5.3.14 Független sebezhetőség vizsgálat (ASVA_VAN.2)

ASVA_VAN.2.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

ASVA_VAN.2.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

ASVA_VAN.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.2.2E Az értékelőnek kereséseket kell végeznie a nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2.3E Az értékelőnek független sebezhetőség vizsgálatot kell végrehajtania az STOE-ra, felhasználva az SST, a biztonsági architektúra leírás, a rendszer interfész specifikáció, a rendszer biztonsági terv, a rendszer-működési biztonsági koncepció és az útmutató dokumentációk által biztosított ismereteket, az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközöket is felhasználva, behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy alap támadó képességgel rendelkező támadó által végrehajtott támadásnak.

1.6 Rendszer összefoglaló előírás

A DBCS rendszer biztonsági filozófiája az alábbiakkal összegezhető:

- a fejlesztés és értékelés lezárásaként előáll egy operációs rendszer és különböző alkalmazás készletek (hash, rgen, dbcs) mesterpéldányai,
- az operációs rendszer és az adott összekapcsolási projekthez kiválasztott alkalmazások munkapéldányai egy pendrive-ra másolódnak,
- a DBCS rendszer egy beépített háttértároló és hálózati kapcsolat nélküli munkaállomáson fut, melyhez minden adatösszekapcsolási projekt esetén egy munkapéldány pendrive kapcsolódik,
- a munkapéldány pendrive-ra kerülnek az alkalmazások kimeneti állományai (eredmények és naplórekordok) is.
- egy live-CD segítségével a kimenti állományokat mobil adathordozóra másolják, és átadják az érintett külső szervezeteknek (adatkezelő, adatkérő),
- az összekapcsolás végén a munkapéldány pendrive teljes tartalmát törlik, a szervezetben az összekapcsolási projektekhez kapcsolódóan a naplóállományokon kívül semmilyen adat nem tárolódik.

A 8. táblázat a (DBCS által felvállalt) fokozott kihatású biztonsági osztály követelményeit tartalmazza, a jobboldali oszlopban feltüntetve azokat a követelményeket is, melyek a DBCS rendszerre nem vonatkoznak (pontosabban automatikusan kielégítettnek tekinthetők a rendszer off-line működése miatt, amint azt 1.5.1 megjegyzési kimutatták).

Követelmények		**Bővítések a fokozott kihatású biztonsági osztályban**	**DBCS-re automatikusan teljesül** (vagy a rendszeren kívül biztosítják)
jele	**elnevezése**		
	Azonosítás és hitelesítés		
AH-1	Azonosítási és hitelesítési szabályzat és eljárásrend	-	
AH-2	Felhasználó azonosítása és hitelesítése	(a)	(a)
AH-3	Eszközök azonosítása és hitelesítése	-	
AH-4	Azonosító kezelés	-	
AH-5	A hitelesítésre szolgáló eszközök kezelése	-	
AH-6	A hitelesítésre szolgáló eszköz visszacsatolása	-	
AH-7	Hitelesítés kriptográfiai modul esetén	-	AH-7
	Hozzáférés ellenőrzése		
HE-1	Hozzáférés ellenőrzési szabályzat és eljárásrend	-	
HE-2	Felhasználói fiókok kezelése	(a), (b), (c), (d)	(b), (d)
HE-3	Hozzáférés ellenőrzés érvényre juttatása	(a)	
HE-4	Információ áramlás ellenőrzés érvényre juttatása	-	
HE-5	A felelősségek szétválasztása	-	
HE-6	Legkisebb jogosultság	-	
HE-7	Sikertelen bejelentkezési kísérletek	-	
HE-8	A rendszerhasználat jelzése	-	HE-8
HE-11	A munkaszakasz zárolása	-	

Követelmények		Bővítések a fokozott kihatású biztonsági osztályban	DBCS-re automatikusan teljesül (vagy a rendszeren kívül biztosítják)
jele	**elnevezése**		
HE-12	A munkaszakasz lezárása	-	HE-12
HE-13	Felügyelet és felülvizsgálat — hozzáférés ellenőrzés	(a)	
HE-14	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek	(a)	
HE-17	Távoli hozzáférés ellenőrzése	(a), (b), (c), (d)	HE-17, (a), (b), (c), (d)
HE-18	A vezeték nélküli hozzáférésre vonatkozó korlátozások	(a)	HE-18, (a)
HE-19	A hordozható és mobil eszközök hozzáférés ellenőrzése	-	HE-19
HE-20	Külső informatikai rendszerek használata	(a)	HE-20, (a)
	Rendszer és kommunikáció védelem		
RV-1	Rendszer és kommunikáció védelmi szabályzat és eljárásrend	-	
RV-2	Alkalmazás szétválasztás	-	
RV-4	Információ maradványok	-	
RV-5	Szolgáltatás megtagadás elleni védelem	-	RV-5
RV-7	A határok védelme	(a), (b), (c), (d), (e)	(a), (b), (c), (d), (e)
RV-8	Az adatátvitel sértetlensége	-	
RV-9	Az adatátvitel bizalmassága	-	
RV-10	A hálózati kapcsolat megszakítása	-	RV-10
RV-12	Kriptográfiai kulcs előállítása és kezelése	-	
RV-13	Jóváhagyott kriptográfia alkalmazása	-	
RV-14	Sértetlenség védelem nyilvános hozzáférés esetén	-	RV-14
RV-15	Telekommunikációs szolgáltatások korlátozása	-	RV-15
RV-17	Nyilvános kulcsú infrastruktúra tanúsítványok	-	RV-17
RV-18	Mobil kód korlátozása	-	RV-18
RV-19	Interneten Keresztüli Hangátvitel (VoIP)	-	RV-19
RV-20	Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)	-	RV-20
RV-22	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	-	RV-22
RV-23	Munkaszakasz hitelessége	-	
	Rendszer és információ sértetlenség		
RS-1	Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend	-	
RS-2	Hibajavítás	(b)	
RS-3	Rosszindulatú kódok elleni védelem	(a), (b)	RS-3: automatikus frissítési lehetőség, (a), (b)
RS-4	Behatolás észlelési eszközök és technikák	(d)	RS-4, (d)
RS-5	Biztonsági riasztások és tájékoztatások	-	RS-5
RS-8	Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem	-	RS-8
RS-9	A bemeneti információra vonatkozó korlátozások	-	
RS-10	A bemeneti információ pontossága, teljessége, érvényessége és hitelessége	-	
RS-11	Hibakezelés	-	
RS-12	A kimeneti információ kezelése és megőrzése	-	
	Naplózás és elszámoltathatóság	bővítés	
NA-1	Naplózási és elszámoltathatósági szabályzat és eljárásrend	-	
NA-2	Naplózandó események	(c)	

Követelmények		Bővítések a fokozott kihatású biztonsági osztályban	DBCS-re automatikusan teljesül (vagy a rendszeren kívül biztosítják)
jele	**elnevezése**		
NA-3	A naplóbejegyzések tartalma	(a)	(a)
NA-4	Napló tárkapacitás	-	
NA-5	Naplózási hiba kezelése	-	NA-5: napló tárkapacitás
NA-6	Napló figyelése, vizsgálata és jelentések készítése	(b)	NA-6, (b)
NA-7	Naplócsökkentés, naplóriport készítés	(a)	NA-7, (a)
NA-8	Időbélyegek	(a)	
NA-9	A napló információk védelme	-	
NA-11	A naplóbejegyzések megőrzése	-	
	Konfiguráció kezelés		
KK-1	Konfiguráció kezelési szabályzat és eljárásrend	-	
KK-2	Alap konfiguráció	(a)	
KK-3	Konfigurációváltozások ellenőrzése	-	
KK-4	A konfigurációváltozások felügyelete	-	
KK-5	A változtatásokra vonatkozó hozzáférés korlátozások	-	
KK-6	Konfigurációs beállítások	-	
KK-7	Legszűkebb funkcionalitás	-	
KK-8	Informatikai rendszer komponens leltár	(a)	
	Speciális kiegészítő elvárások		
SK-1	Adatbázis elemek összekapcsolása		
SK-2	Minősített hash függvény		
SK-3	Véletlenített hash függvény		
SK-4	Visszaállíthatatlan törlés		

8. táblázat: A DBCS rendszerre vonatkozó követelmények

Az alábbiak arra vonatkozóan adnak egy magas szintű áttekintést, hogy az egyes követelményeket hogyan (milyen eszközökkel) teljesíti a rendszer. A részleteket az egyes fejlesztői bizonyítékok tartalmazzák, illetve az értékelés ellenőrzi.

1.6.1 Az azonosításra és hitelesítésre vonatkozó követelmények teljesítési módja

/Teljesítendő követelmények: AH-1, AH-2, AH-3, AH-4, AH-5, AH-6/

A DBCS rendszer biztonsági funkcionalitását részletesen leíró *Rendszer interfész specifikáció* tartalmazza az azonosításra és hitelesítésre vonatkozó szabályzatot, az ehhez kapcsolódó ellenőrzések megvalósítását pedig az *Eljárásrend* segíti (AH-1).

Az operációs rendszer felhasználó név és jelszó alapján egyedileg azonosítja és hitelesíti a felhasználókat (AH-2).

A rendszergazda biztosítja a felhasználói nevek megfelelő kezelését (AH-4), a rendszergazda és a jelszó tulajdonosa pedig együttesen biztosítják a jelszó megfelelő kezelését (AH-5).

Az operációs rendszer megvalósítja a jelszó védett visszacsatolását a felhasználó hitelesítési kísérlete során (AH-6).

Eljárásrendi intézkedésekkel azonosítják és hitelesítik az operációs rendszer mester- és munkapéldányát tartalmazó eszközt, a célszoftverek mesterpéldányát tartalmazó eszközt, valamint a külső rendszerekkel (adatkérő, adatkezelők) való kapcsolathoz és a naplóállományok megőrzésére használt mobil adathordozókat (AH-3).

1.6.2 A hozzáférés ellenőrzésre vonatkozó követelmények teljesítési módja

/Teljesítendő követelmények: HE-1, HE-2 (a) (c), HE-3 (a), HE-4, HE-5, HE-6, HE-7, HE-11, HE-13 (a), HE-14 (a)/

A DBCS rendszer biztonsági funkcionalitását részletesen leíró *Rendszer interfész specifikáció* tartalmazza a hozzáférés ellenőrzésre vonatkozó szabályzatot, az ehhez kapcsolódó ellenőrzések megvalósítását pedig az *Eljárásrend* segíti (HE-1).

Az operációs rendszer biztosítja, hogy a DBCS rendszerben csak sikeres azonosítás és hitelesítés után lehet bármilyen más tevékenységet végrehajtani (HE-14).

Eljárásrendi intézkedések egy adott korlátot (3) juttatnak érvényre egy felhasználó egymást követő sikertelen bejelentkezési kísérleteire (HE-7).

Az operációs rendszer az egyes szerepkörökhöz (rendszergazda, rendszerüzemeltető, rendszervizsgáló) kijelölt hozzáférési jogosultságokon keresztül szétválasztja a felelősségeket (HE-5). Az operációs rendszer azt is érvényre juttatja, hogy minden felhasználó (illetve a felhasználó nevében fellépő eljárás) csak a feladatai végrehajtásához szükséges jogosultsággal és hozzáférési lehetőséggel rendelkezik (HE-6).

A rendszergazda kezeli a felhasználói fiókokat (HE-2).

Eljárásrendi intézkedések, valamint az operációs rendszer jogosultság ellenőrző mechanizmusai biztosítják, hogy a rendszerhez való hozzáférés és az információ áramlás ellenőrzés a kiosztott jogosultságokat juttatja érvényre (HE-3, HE-4).

Eljárásrendi intézkedés a sikeres bejelentkezést követő 30 perces inaktivitás után zárolja a munkaszakaszt, s a rendszerhez való további hozzáférést mindaddig, amíg a felhasználó nem azonosítja és hitelesíti újra magát (HE-11).

Eljárásrendi intézkedések felügyelik és felülvizsgálják a felhasználók tevékenységét az informatikai rendszer hozzáférés ellenőrzése érvényre juttatása és használata tekintetében. Ennek alapja az automatikus naplózási mechanizmus, illetve a naplóállományok utólagos feldolgozása és elemzése (HE-13).

1.6.3 A rendszer és kommunikáció védelmére vonatkozó követelmények teljesítési módja

/Teljesítendő követelmények: RV-1, RV-2, RV-4, RV-7, RV-8, RV-9, RV-12, RV-13, RV-23/

A DBCS rendszer biztonsági funkcionalitását részletesen leíró *Rendszer interfész specifikáció* tartalmazza a rendszer és kommunikáció védelmi szabályzatot, az ehhez kapcsolódó ellenőrzések megvalósítását pedig az *Eljárásrend* segíti (RV-1).

Az operációs rendszer és eljárásrendi intézkedések biztosítják, hogy a rendszerüzemeltetők által elérhető funkcionalitás elkülönül a rendszergazda által elérhető adminisztratív funkcionalitástól (RV-2).

Az operációs rendszer tartomány szétválasztási, önvédelmi és megkerülhetetlenséget biztosító mechanizmusai eljárásrendi intézkedésekkel kiegészítve megakadályozzák a megosztott rendszer erőforrások útján történő jogosulatlan és véletlen információáramlást (RV-4).

A célszoftverek figyelik és ellenőrzik a külső határokon történő kommunikációkat (RV-7).

A továbbított információk sértetlenségét és bizalmasságát eljárásrendi intézkedések biztosítják (RV-8, RV-9).

Az operációs rendszer automatikus rejtjelezéssel védi a felhasználókat hitelesítő jelszavakat (RV-12).

Az operációs rendszer megkerülhetetlenséget biztosító és jogosultság-kezelő mechanizmusai eljárásrendi intézkedésekkel kiegészítve biztosítják a munkaszakaszok hitelességét (RV-23).

1.6.4 A rendszer és információ sértetlenségére vonatkozó követelmények teljesítési módja

/Teljesítendő követelmények: RS-1, RS-2 (b), RS-3, RS-9, RS-10, RS-11, RS-12/

A DBCS rendszer biztonsági funkcionalitását részletesen leíró *Rendszer interfész specifikáció* tartalmazza a rendszer és kommunikáció sértetlenségére vonatkozó szabályzatot, az ehhez kapcsolódó ellenőrzések megvalósítását pedig az *Eljárásrend* segíti (RS-1).

A rendszer informatika biztonsági értékelése során feltárt valamennyi hibát kijavították. Eljárásrendi intézkedések biztosítják, hogy a rendszer továbbfejlesztett változatait is értékelni fogják biztonsági szempontból, az esetlegesen feltárt hibákat pedig kijavítják (RS-2).

A biztonsági értékelés ellenőrzése, valamint a rendszer off-line jellege biztosítja a rosszindulatú kódok elleni védelmet (RS-3).

Az operációs rendszer és eljárásrendi intézkedések biztosítják, hogy csak a rendszerüzemeltetők működtethetik a célszoftvereket, és csak a rendszergazda érheti el az adminisztratív funkciókat (RS-9).

A célszoftverek ellenőrző mechanizmusai és eljárásrendi intézkedések biztosítják az információ bemenetek pontosságát, teljességét, érvényességét és hitelességét (RS-10).

Az operációs rendszer és a célszoftverek megfelelő módon azonosítják és kezelik a hibákat (RS-11).

Eljárásrendi intézkedések biztosítják a kimeneti információ megfelelő kezelését és megőrzését (RS-12).

1.6.5 A naplózásra és elszámoltathatóságra vonatkozó követelmények teljesítési módja

/Teljesítendő követelmények: NA-1, NA-2 (c), NA-3, NA-4, NA-5, NA-8 (a), NA-9/

A DBCS rendszer biztonsági funkcionalitását részletesen leíró *Rendszer interfész specifikáció* tartalmazza a naplózásra és elszámoltathatóságra vonatkozó szabályzatot, az ehhez kapcsolódó ellenőrzések megvalósítását pedig az *Eljárásrend* segíti (NA-1).

Az operációs rendszer és a célszoftverek olyan naplóbejegyzéseket állítanak elő, melyek alapján utólag ki lehet mutatni, hogy milyen események történtek, ezek az események miből származtak és milyen eredménnyel jártak (NA-2, NA-3).

A tervezés során kellő méretű (4 Gbyte-os) PEN drive-ról gondoskodtak, hogy minden esetben elférjen rajta a naplóállomány (NA-4).

A naplóbejegyzésekbe belekerül a rendszeridő, s ennek pontosságát a rendszergazda rendszeres beállítással biztosítja (NA-8, (a)).

Naplózási hiba esetén a teljes adatbázis összekapcsolási folyamat ismételten végrehajtásra kerül (NA-5).

A DBCS rendszer SHA-1 hash értékkel védi az adathordozóra másolt naplóállományokat. A naplóállományokat tartalmazó adathordozót adminisztratív intézkedések védik a jogosulatlan

hozzáféréssel, módosítással és törléssel szemben (NA-9). A rendszervizsgáló a naplóbejegyzéseket 5 évig megőrzi (NA-11).

1.6.6 A konfiguráció kezelésre vonatkozó követelmények teljesítési módja

/Teljesítendő követelmények: KK-1, KK-2 (a), KK-3, KK-4, KK-5, KK-6, KK-7, KK-8 (a)/

A DBCS rendszer biztonsági funkcionalitását részletesen leíró *Rendszer interfész specifikáció* tartalmazza a naplózásra és elszámoltathatóságra vonatkozó szabályzatot, az ehhez kapcsolódó ellenőrzések megvalósítását pedig az *Eljárásrend* segíti (KK-1).

A csak a szükséges lehetőségeket nyújtó (hálózatra kapcsolódás lehetőségét letiltó) minimális alap konfigurációt (KK-7) dokumentálták és tartják karban (KK-2). Az alap konfiguráció meghatározás egyúttal a rendszer komponenseinek egy aktuális leltárát is tartalmazza (KK-8).

Eljárásrendi intézkedések biztosítják a rendszerben történt változások dokumentálását és ellenőrzését (KK-3), a rendszer (konfigurációs) változtatásaira vonatkozó hozzáférési korlátozások érvényre juttatását (KK-5).

Független informatika biztonsági értékelések biztosítják a konfigurációváltozások felügyeletét (KK-4), biztonsági hatásvizsgálatot végezve újabb mesterpéldányok készítése esetén.

Eljárásrendi intézkedések biztosítják a rendszer kötelező, lehető legkorlátozóbb konfigurációs beállítását és ezek dokumentálását (KK-6).

1.6.7 A speciális kiegészítő elvárások teljesítési módja

A dbcs (összekapcsoló) program biztosítja az alábbiakat:

- a különböző adatkezelők adatbázisaiból az azonos alanyra vonatkozó adatelemeket összekapcsolja,
- az összekapcsolás alapja egy olyan személyazonosító adat (adóazonosító jel, társadalombiztosítási azonosító jel, személyazonosító jel, vagy név és lakcím együttese), melynek kezelésére valamennyi adatkezelő jogosult,
- az összekapcsolás megvalósítása az alapját képező személyazonosító adatra (a hash függvénnyel) számolt anonim kapcsolati kóddal történik,

biztosítva ezzel SK-1 teljesítését.

A hash függvény készlet olyan hash függvényeket tartalmaz, melyekre igazoltan (külön kriptográfiai vizsgálat pozitív minősítési eredménye szerint) teljesülnek az alábbiak:

- egyirányúság,
- szigorú lavina-hatás,
- ütközés-ellenállóság,
- hossznövekedés elleni támadások elleni ellenállás,
- „véletlenszerű” leképezésként való viselkedés,
- nehezen invertálhatóság rövid bemenő adatra,
- a bemenetek teljes kipróbálásának kizárása rövid bemenő adatra,

biztosítva ezzel SK-2 teljesítését.

Az rgen (véletlen generáló) program biztosítja az alábbiakat:

- a kiválasztott hash függvényhez egyedi, véletlenszerűen megállapított elemeket is generál,
- a véletlen generálásra megfelelő módon kerül sor,

- a generált véletlen rendelkezik legalább 100 bit szabadságfokkal,

biztosítva ezzel SK-3 teljesítését.

Az összekapcsolási projekt végén az operációs rendszer és a célszoftverek munkapéldányát tartalmazó adathordozó tartalmának teljes fizikai törlése kizárja az adathordozón átmenetileg tárolt alábbi információk utólagos megismerhetőségét:

- a hash-függvény paraméterezéséhez generált véletlen elemek,
- a kapcsolati kódok (az összekapcsolást megalapozó hash értékek),

biztosítva ezzel SK-4 teljesítését.

2. A biztonsági tartományok jellemzése

A DBCS rendszer egységes biztonsági tartományt képvisel (nem osztható olyan különböző biztonsági tartományokra, melyek üzemeltetési környezetében jelentős eltérések lennének).

Következésképp nincs szükség az elkülönülő biztonsági tartományok külön jellemzésére.

3. Hivatkozások, fogalmak és rövidítések

3.1 Hivatkozások

A jelen rendszer biztonsági előirányzatban megfogalmazottak az alábbi mértékadó dokumentumokon alapulnak:

[1] 2007. évi CI. törvény a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról

[2] 335/2007. (XII. 13.) kormányrendelet a döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 2007. évi CI. törvény végrehajtásáról

[3] Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) - Part 1: Introduction and general model - Part 2: Security functional components - Part 3: Security assurance components

[4] A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA), v1.0, 2008 június

[5] A KIB 25. számú ajánlása - 2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) v1.0, 2008 június

[6] A KIB 25. számú ajánlása – 25/2-5 segédlet: MIBÉTS - Értékelési módszertan, v1.0, 2008 június

[7]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, megtalálható az alábbi helyen: http://kovetelmenytar.complex.hu)

[8]: IT biztonsági műszaki követelmények a különböző biztonsági szintekre, BME IK, 2008.

[9]: Útmutató az IT biztonsági szintek meghatározásához BME IK, 2008.

3.2 Fogalom-meghatározások

Jelen rendszer biztonsági előirányzat az alábbi fogalmakat az alábbi értelemben használja:

Anonim kapcsolati kód: Az ugyanazon személyre vonatkozó személyazonosító adatokból olyan, véletlenszerű elemet is tartalmazó módszerrel képzett karaktersor, amellyel ugyanazokból az adatokból mindig ugyanaz a karaktersor jön létre, de amely eredményeképpen létrejött karaktersorból a személyazonosító adatok nem állíthatók helyre.

Biztonsági cél: Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

Biztonsági követelmények: Az informatikai biztonsági célok lebontása biztonsági funkcionalitásra (SFR) és garanciára (SAR) vonatkozó szakmai követelmények egy összességére, melyek az értékelés tárgyára és annak üzemeltetési környezetére vonatkoznak.

Garancia: Biztosíték arra nézve, hogy egy egyed megfelel a rá vonatkozó biztonsági céloknak.

Garanciaosztály: Garanciacsaládok egy olyan csoportja, melyek közös feladatokhoz kapcsolódnak. A jelen dokumentumban meghatározott garanciaosztályok az alábbiak: Rendszer biztonsági előirányzat (ASST), Rendszer fejlesztés (ASDV), Rendszer útmutató dokumentumok (ASGD), Rendszer konfiguráció kezelés (ASCM), Rendszer tesztelés (ASTE) és Rendszer sebezhetőség felmérés (ASVA).

Interfész: Különböző informatikai rendszerek közötti, illetve egy informatikai rendszer és felhasználói közötti adatátadást megvalósító rendszerkomponens.

Rendszer biztonsági előirányzat (SST): Biztonsági követelmények és előírások olyan összessége, amelyet egy értékelt rendszerre, az értékelés alapjaként használnak.

Rendszer biztonsági funkcionalitás (SSF): Az értékelt rendszer mindazon részei, amelyekre a rendszer biztonsági szabályzatának helyes érvényre juttatásához támaszkodni kell, illetve lehet.

Rendszer biztonsági szabályzat: Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy informatikai rendszer biztonságos működtetéséhez a rendszer tulajdonosa állít fel.

Rendszer értékelési garanciacsomag (SAP): Garancia-összetevőkből álló csomag, amelyek egy-egy pontot képviselnek egy előre meghatározott garanciális skálán. A [7] által meghatározott rendszer értékelési módszertan a garanciális skála alábbi három szintjét különbözteti meg: alap (SAP-A), fokozott (SAP-F), kiemelt (SAP-K).

Szervezeti biztonsági szabályzat (OSP): Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy szervezet saját biztonságos működtetéséhez állít fel.

Szolgáltató (informatikai) rendszer: Egy konkrét informatikai elrendezés meghatározott céllal és üzemeltetési környezettel.

Támadó képesség: Támadás esetén annak érzékelt lehetősége, hogy a támadás sikeres lesz, a támadó szaktudásával, erőforrásaival és motivációjával kifejezve. (Lehetséges szintjei: alap, megemelt-alap, közepes, magas, a [7] által meghatározott rendszer értékelési módszertan szerint lehetséges szintjei: alap, megemelt-alap.)

Termék: Informatikai szoftver, förmver és/ vagy hardver által alkotott csomag, amelyek adott használatra vagy különböző szolgáltató rendszerekbe való beépítésre tervezett funkciókészletet biztosítanak.

3.3 Rövidítések

Jelen rendszer biztonsági előirányzat az alábbi táblázatban megadott rövidítéseket használja:

Rövidítés	Angol	Magyar
A	Assumption	Feltételezés
ASCM	Assurance: System Configuration Management	"Rendszer konfiguráció kezelés" garanciaosztály
ASCM_SBC	ASCM: System Base-Configuration	Rendszer alap konfiguráció garanciacsalád
ASCM_ECC	ASCM: Evaluated and Certified Components	Értékelt és tanúsított komponensek garanciacsalád
ASDV	Assurance: System Development	"Rendszer fejlesztés" garanciaosztály
ASDV_ARC	ASDV: Security Architecture	Biztonsági architektúra garanciacsalád
ASDV_OSC	ASDV: Operational Security Concepts	Rendszer-működési biztonsági koncepció garanciacsalád
ASDV_SDS	ASDV: STOE Design	STOE terv garanciacsalád
ASDV_SIS	ASDV: System Interface Specification	Rendszer interfész specifikáció garanciacsalád
ASGD	Assurance: System Guidance Documents	"Rendszer útmutató dokumentumok" garanciaosztály
ASGD_CON	ASGD: Configuration Guidance	Konfigurálási útmutató garanciacsalád
ASGD_OPE	ASGD: Operational User Guidance	Üzemeltetési útmutató garanciacsalád
ASGD_PRE	ASGD: Preparative guidance	Előkészítő útmutató garanciacsalád
ASTE	Assurance: Security Tests	"Rendszer tesztelés" garanciaosztály
ASTE_COV	ASTE: Coverage	Lefedettség garanciacsalád
ASTE_DPT	ASTE: Depth	Mélység garanciacsalád
ASTE_FUN	ASTE: Functional Tests	Funkcionális tesztek garanciacsalád
ASTE_IND	ASTE: Independent Testing	Független tesztelés garanciacsalád
ASVA	Assurance: System Vulnerability Assessment	"Rendszer sebezhetőség felmérés" garanciaosztály
ASVA_VAN	ASTE: Vulnerability Analysis	Sebezhetőségi elemzés garanciacsalád
CC	Common Criteria	Közös szempontok
CEM	Common Evaluation Methodology	Közös értékelési módszertan
CM	Configuration Management	Konfiguráció kezelés
DBCS	Data Base Connection system	Adatbázisok anonimizált összekapcsolását megvalósító rendszer
IT	Information Technology	Információs technológia, informatika
O	Object	(Biztonsági) cél (az STOE-re)
OE	Object for the Environment	(Biztonsági) cél az üzemeltetési környezetre
OSP	Organisational Security Policy	Szervezeti biztonsági szabályzat
SAP	Security Assurance Package	Rendszer garanciacsomag
SAR	Security Assurance Requirement	Garanciális biztonsági követelmény
SFR	Security Functional Requirement	Funkcionális biztonsági követelmény
SSF	STOE Security Functionality	Rendszer biztonsági funkcionalitás
SST	System Security Target	Rendszer biztonsági előirányzat
STOE	System Target of Evaluation	Rendszer értékelés tárgya
T	Threat	Fenyegetés