TANÚSÍTÁSI JELENTÉS

SIEMENS SZÁMLA ARCHIVÁLÓ RENDSZER

2015.03.01-i állapot

HUNG-TJ-DA-002-2015

Verzió:	1.0	
Fájl:	DA_TJ_002_Siemens_v10.pdf	
Minősítés:	Nyilvános	
Oldalak:	22	

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2015.03.25	A szerkezet felállítása
v0.2	2015.04.08	Belső egyeztetésre kiadott verzió
v0.9	**2015.04.10**	**Külső egyeztetésre kiadott verzió**
v1.0	2015.04.15	Végleges verzió

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft.
Tanúsítási divízió

Tartalomjegyzék

1 A tanúsítás tárgyának azonosítása

STOE név:	SIEMENS SZÁMLA ARCHIVÁLÓ RENDSZER
STOE verzió:	2015.03.01-i állapot
Rendszer integrátor:	ATOS SE – France, River Ouest 80, Quai Voltaire 95877 Bezons
Rendszer működtető:	Siemens Zrt.– 1143 Budapest, Gizella út 51-57.
Rendszer üzemeltető:	ATOS SE – France, River Ouest 80, Quai Voltaire 95877 Bezons
Rendszer értékelő:	Hunguard Kft. Értékelési Divízió 1123. Budapest, Kékgolyó u. 6. 5. em. 6.

2 A tanúsítás jellemzése

2.1 Az alkalmazott tanúsítási és értékelési módszer

Az alábbiakban az értékelés és tanúsítás során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

MIBÉTS:2009 rendszerértékelési és tanúsítási módszertan

Az STOE értékelésére a MIBÉTS 2009 Rendszerekre vonatkozó értékelési módszertan és a MIBÉTS 2009 Útmutató rendszer értékelőknek mértékadó dokumentumokban meghatározott, rendszerekre vonatkozó értékelési módszertant alkalmaztuk, az alábbi pontosításokkal:

- a rendszer értékelés típusa[1]: **kezdeti**
- a rendszer értékelés garanciaszintje[2]: **MIBÉTS fokozott (SAP-F)**

A rendszer értékelés keretében elvégzett fő feladat-csoportok az alábbiak voltak:

a) a rendszer biztonsági előirányzat értékelése,
b) a rendszer biztonsági architektúrájának értékelése,
c) a rendszer telepítési és üzemeltetési útmutatóinak a vizsgálata,
d) a rendszer konfiguráció vizsgálata,
e) a rendszer biztonsági tesztelése,
f) a rendszer sebezhetőség vizsgálata.

Kiegészítő értékelések

Jelen kezdeti rendszer értékelés alapvetően annak megállapítására irányult, hogy az STOE a zártság követelményeit kielégítik-e.

Egy elektronikus információs rendszer **zárt**, ha

1. Az informatikai rendszer zárt, teljes körű, folytonos és kockázatokkal arányos védelmet biztosít a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából /lásd 2013. L. törvény – a továbbiakban IBTV - 1. § 15/, az alábbi értelmezések mellett:

- zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem / IBTV (1. § 48) /,
- teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem / IBTV (1. § 44) /,
- folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem / IBTV (1. § 21) /,
- kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével / IBTV (1.§ 31) /.

[1] A rendszer értékelés típusai: kezdeti, tervezett felülvizsgálati, rendkívüli felülvizsgálati, megismételt kezdeti.
[2] A rendszer értékelés lehetséges garanciaszintjei: MIBÉTS alap (SAP-A), MIBÉTS fokozott (SAP-F) és MIBÉTS kiemelt (SAP-K) rendszer értékelési garanciacsomag.

Az elvárásoknak megfelelő részletes követelményrendszer megtalálható az IBTV-hez kapcsolódó 77/2013. (XII.19.) NFM rendelet 3.-4. mellékletében.

2. A védelem fenti általános elvárásai mellett az informatikai rendszer működtetésének teljes életciklusában folyamatosan teljesülnek az alábbiak:

- a jogosult általános (emberek és program entitások) és privilegizált (speciális jogokkal felruházott) felhasználók (pl. rendszergazdák) kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhetnek a védendő információkhoz és az azokat kezelő rendszer elemeihez, kezdeményezhetnek aktivitásokat, valamint kizárólag meghatározott privilegizált felhasználók adhatnak szabályozott szerepkörüknek megfelelően és ellenőrzött módon hozzáférési jogosultságokat;
- a rendszer megfelelő műszaki és eljárásrendi megoldásokkal nyomon követi a védendő információk minden változtatását, melyek biztosítják, hogy még a jogosult általános és privilegizált felhasználók sem tudják törölni vagy módosítani a napló vagy egyéb nyomon követést biztosító információkat;
- az informatikai rendszer összes külső interfésze szabályozott és kontrollált;
- a szabályozások és eljárások garantálják a rendszer biztonsági szintjének folyamatos fenntartását (szoftverfrissítések, üzemeltetés,…).

A Rendszer Biztonsági Előirányzat a 77/2013. (XII. 19.) NFM rendeletnek való megfelelőséget állítja:

- az 1-es biztonsági szintre vonatkozó adminisztratív védelmi intézkedések,
- a 2-es biztonsági szintre vonatkozó fizikai védelmi intézkedések,
- a bizalmasság, sértetlenség és rendelkezésre állás szempontjából szerint 3-as biztonsági osztályba sorolt elektronikus információs rendszerekre vonatkozó logikai védelmi intézkedések.

A Rendszer Biztonsági Előirányzat a biztonsági osztályba sorolást a logikai védelmi intézkedések tekintetében az alábbiakban határozta meg:

A számlázó rendszer biztonsági osztálya a bizalmasság szempontjából: **3**
A számlázó rendszer biztonsági osztálya a sértetlenség szempontjából: **3**
A számlázó rendszer biztonsági osztálya a rendelkezésre állás szempontjából: **3**

A Rendszer Biztonsági Előirányzat környezeti biztonsági célként fogalmazza meg az STOE környezetét képező adminisztratív és fizikai védelmi intézkedéseket az alábbi biztonsági osztályba sorolás alapján:

A rendszer biztonsági osztálya az adminisztratív védelmi intézkedések szempontjából: **1**
A rendszer biztonsági osztálya a fizikai védelmi intézkedések szempontjából: **2**

A fenti biztonsági osztályokba soroláshoz tartozó követelmények teljesülése a zártságot biztosítják.

2.2 A tanúsításhoz felhasznált értékelési dokumentumok azonosítása

Rendszer Biztonsági Előirányzat - SIEMENS SZÁMLA ARCHIVÁLÓ RENDSZER, v1.0, SST_Siemens_archivalas_v1.0.pdf

Rendszer értékelési jelentés - SIEMENS SZÁMLA ARCHIVÁLÓ RENDSZER 2015.03.01.-i állapot, v1.0, SETR_Siemens_archivalas_v1.0.pdf

ISO/IEC27001:2005 tanúsítvány; azonosító:2013-006; kibocsátó: AtoS SA

3 Az értékelés eredményei

3.1 A MIBÉTS 2009 értékelés eredményei

3.1.1 A rendszer biztonsági előirányzat értékelése

A rendszer biztonsági előirányzat tartalma alapján megfelel a MIBÉTS rendszer értékelési módszertan SST-re (System Security Target) megfogalmazott elvárásainak.

Az SST egy belső ellentmondásoktól mentes, teljes és egymást erősítő biztonsági követelményrendszert határoz meg, egyúttal magas szinten át is tekinti, hogy a Siemens archiválási rendszer hogyan teljesíti a biztonsági követelményeket.

3.1.2 A rendszer fejlesztésének értékelése

A kialakított rendszer megfelel a MIBÉTS rendszer értékelési módszertan rendszer fejlesztés garanciaosztály elvárásainak (SAP-F fokozott garanciacsomag mellett).

A rendszer tervezése és kiépítése során a biztonságos működés és a magas rendelkezésre állás folyamatosan kiemelt szempont volt. A helyszíni vizsgálatok során megállapítást nyert, hogy a kiépített rendszer jól dokumentált, átgondolt, biztonsági szempontból megalapozott. Az üzemeltetők ismerik, és magas szinten használják a teljes szervezetre nézve meglévő legkorszerűbb technológiákat (pl. PKI, authentication, authorization, accounting, audit). Az alkalmazás a belső kommunikációra is védett protokollokat használ (SSL).

3.1.3 A rendszer konfigurálási és üzemeltetési útmutatóinak a vizsgálata

A konfigurálási eljárások és az üzemeltetési útmutatók megfelelnek a MIBÉTS rendszer értékelési módszertan rendszer útmutató dokumentumok és rendszer konfiguráció kezelés garanciaosztály elvárásainak (SAP-F fokozott garanciacsomag mellett).

A rendszer konfigurálása és üzemeltetése egységes és jól dokumentált. A dokumentációk alapján a konfiguráció biztonságosan megismételhető, ellenőrizhető. Az eljárásrend dokumentációk a szervezet egészére vonatkoznak, magas színvonalúak.

A megvalósított konfiguráció támogatja a biztonságos üzemeltetést (megerősített, nyilvános kulcsú távoli hozzáférés – SSO PKI kártya alapján; szigorú tűzfal szabályok, gyártó által biztosított megerősített operációs rendszer; kiépített felügyeleti rendszer, amely a rendszer működése során felmerülő hibákra azonnal riaszt).

3.1.4 A rendszer biztonsági tesztelése

Az értékelők a rendszer működésével és üzemeltetésével kapcsolatban teszteket hajtattak végre, mely eredményeket dokumentáltak. A tesztelés keretében egy számla digitalizálásától kezdve, az archivált anyag Saperion-ba érkezéséig végig követék a folyamatot.

A rendszertesztelés megfelel a MIBÉTS rendszer értékelési módszertan rendszertesztelés garanciaosztály elvárásainak (SAP-F fokozott garanciacsomag mellett).

3.1.5 A rendszer sebezhetőség vizsgálata

Mind az SAP, mind a Saperion rendszerek megtalálhatóak nyilvános sebezhetőségi adatbázisokban. Az alkalmazott verziók nem tartalmaznak ismert sebezhetőséget. A rendszer harmadik fél által fejlesztett komponenst nem tartalmaz.

A működtető környezet operációs rendszerei az SAP és a SAPERION sebezhetőségeinek kivédésére az üzemeltetők folyamatosan frissítették a környezetet a legújabb verzióra, amelyben a hibák javításra kerülnek.

A vizsgálat alapján kijelenthető, hogy a kialakított rendszer megfelel a MIBÉTS rendszer értékelési módszertan rendszer sebezhetőség felmérés garanciaosztály elvárásainak (SAP-F fokozott garanciacsomag mellett).

3.2 A 77/2013. (XII. 19.) NFM rendeletnek való megfeleltetés eredményei

3.2.1 Konfigurációkezelés

Azonosító	Intézkedés, értékelés
CM-1	**3.3.1.1 Konfigurációkezelési eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
CM-2	**3.3.1.2 Alapkonfiguráció** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-3	**3.3.1.3 A konfigurációváltozások felügyelete, változáskezelés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit, Interjú*
CM-3 (2)	**3.3.1.3 Előzetes tesztelés és megerősítés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-4	**3.3.1.4 Biztonsági hatásvizsgálat** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-6	**3.3.1.6 Konfigurációs beállítások** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
CM-7	**3.3.1.7 Legszűkebb funkcionalitás** *Döntés: megfelelt* *Vizsgálati módszerek: Audit, Interjú*
CM-8	**3.3.1.8 Elektronikus információs rendszerelem leltár** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

CM-10	**3.3.1.10 A szoftverhasználat korlátozásai** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-11	**3.3.1.11 A felhasználó által telepített szoftverek** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

3.2.2 Üzletmenet folytonosság

Azonosító	Intézkedés, értékelés
CP-1	**3.3.2.1 Üzletmenet folytonosságra vonatkozó eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
CP-2	**3.3.2.2 Üzletmenet folytonossági terv informatikai erőforrás kiesésekre** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
CP-3	**3.3.2.3 A folyamatos működésre felkészítő képzés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
CP-9	**3.3.2.8 Az elektronikus információs rendszer mentései** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
CP-10	**3.3.2.9 Az elektronikus információs rendszer helyreállítása és újraindítása** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

3.2.3 Rendszer Karbantartás

Azonosító	Intézkedés, értékelés
MA-1	**3.3.3.1 Rendszer karbantartási eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
MA-2	**3.3.3.2 Rendszeres karbantartás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
MA-5	**3.3.3.5 Karbantartók** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

3.2.4 Adathordozók védelme

Azonosító	Intézkedés, értékelés
MP-1	**3.3.4.1 Adathordozók védelmére vonatkozó eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
MP-2	**3.3.4.2 Hozzáférés az adathordozókhoz** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
MP-6	**3.3.4.6 Adathordozók törlése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
MP-7	**3.3.4.7 Adathordozók használata** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

3.2.5 4.6.5 Azonosítás és hitelesítés

Azonosító	Intézkedés, értékelés
IA-1	**3.3.5.1 Azonosítási és hitelesítési eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
IA-2	**3.3.5.2 Azonosítás és hitelesítés (belső felhasználók)** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-2 (1)	**3.3.5.2.2 Hálózati hozzáférés privilegizált fiókokhoz** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-4	**3.3.5.4 Azonosító kezelés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-5	**3.3.5.5 A hitelesítésre szolgáló eszközök kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
IA-6	**3.3.5.6 A hitelesítésre szolgáló eszköz visszacsatolása** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

IA-7	**3.3.5.7 Hitelesítés kriptográfiai modul esetén** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-8	**3.3.5.8.1 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-H	**3.3.5.8.2 Hitelesítésszolgáltatók tanúsítványának elfogadása** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

3.2.6 Hozzáférés ellenőrzés

Azonosító	Intézkedés, értékelés
AC-1	**3.3.6.1 Hozzáférés ellenőrzési eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AC-2	**3.3.6.2 Felhasználói fiókok kezelése** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AC-3	**3.3.6.3 Hozzáférés ellenőrzés érvényesítése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-7	**3.3.6.7 Sikertelen bejelentkezési kísérletek** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-8	**3.3.6.8 A rendszerhasználat jelzése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-14	**3.3.6.12 Azonosítás/hitelesítés nélkül engedélyezett tevékenységek** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-17	**3.3.6.13 Távoli hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-18	**3.3.6.14 Vezeték nélküli hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

AC-19	**3.3.6.15 Mobil eszközök hozzáférés ellenőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-20	**3.3.6.16 Külső elektronikus információs rendszerek használata** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-22	**3.3.6.18 Nyilvánosan elérhető tartalom** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

3.2.7 Rendszer- és információsértetlenség

Azonosító	Intézkedés, értékelés
SI-1	**3.3.7.2 Rendszer- és információsértetlenségre vonatkozó eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
SI-2	**3.3.7.3 Hibajavítás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SI-3	**3.3.7.4 Kártékony kódok elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SI-4	**3.3.7.5 Az elektronikus információs rendszer felügyelete** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SI-5	**3.3.7.6 Biztonsági riasztások és tájékoztatások** *Döntés: megfelelt* *Vizsgálati módszerek: Audit, Interjú*
SI-12	**3.3.7.12 A kimeneti információ kezelése és megőrzése** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*

3.2.8 Naplózás

Azonosító	Intézkedés, értékelés
AU-1	**3.3.8.1 Naplózási eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AU-2	**3.3.8.2 Naplózható események** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-3	**3.3.8.3 Naplóbejegyzések tartalma** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-12	**3.3.8.12 Naplógenerálás** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AU-4	**3.3.8.4 Napló tárkapacitás** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-5	**3.3.8.5 Naplózási hiba kezelése** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AU-6	**3.3.8.6 Naplóvizsgálat és jelentéskészítés** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AU-8	**3.3.8.8 Időbélyegek** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-9	**3.3.8.9 A naplóinformációk védelme** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
AU-11	**3.3.8.11 A naplóbejegyzések megőrzése** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*

3.2.9 Rendszer- és kommunikációvédelem

Azonosító	Intézkedés, értékelés
SC-1	**3.3.9.1 Rendszer- és kommunikációvédelmi eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
SC-5	**3.3.9.5 Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-7	**3.3.9.6 A határok védelme** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SC-12	**3.3.9.10 Kriptográfiai kulcs előállítása és kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SC-13	**3.3.9.11 Kriptográfiai védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SC-15	**3.3.9.12 Együttműködésen alapuló számítástechnikai eszközök** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SC-20	**3.3.9.16 Biztonságos név/cím feloldó szolgáltatások (hiteles forrás)** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SC-21	**3.3.9.17 Biztonságos név/cím feloldó szolgáltatás (gyorsító táras)** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SC-22	**3.3.9.18 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-39	**3.3.9.22 A folyamatok elkülönítése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

3.2.10 Biztonsági események kezelése

Azonosító	Intézkedés, értékelés
IR-1	**3.3.10.1 Biztonsági eseménykezelési eljárásrend** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
IR-2	**3.3.10.2 Képzés a biztonsági események kezelésére** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
IR-4	**3.3.10.4 A biztonsági események kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-5	**3.3.10.5 A biztonsági események figyelése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
IR-6	**3.3.10.6 A biztonsági események jelentése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-7	**3.3.10.7 Segítségnyújtás a biztonsági események kezeléséhez** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-8	**3.3.10.8 Biztonsági eseménykezelési terv** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

3.3 Következtetések

A rendszer értékelés fő következtetése az alábbi:

A SIEMENS számla archiváló rendszere megfelel a rendszer biztonsági előirányzatában meghatározott biztonsági követelményeknek, az értékelési jelentésben azonosított maradvány kockázatok mellett. Az archiválandó adatok formátuma PDF vagy XML, PDF esetén beágyazott CSV, TXT, XML tartalom lehetséges. Ezen szabványos formátumok megjeleníthetőségét az alkalmazott konfigurációkezelő képességek folyamatosan garantálják.

Ennek alapján kijelenthetők az alábbiak:

1. Az archiváló rendszere számlázó rendszer biztosítja a rendszerelemek zártságát és megakadályozza az archiváló rendszerhez, valamint az archivált információk észrevétlen módosítását.
2. Az archiváló rendszer (a logikai védelmi intézkedések tekintetében) megfelel az általános információbiztonsági zártsági követelményeknek.

A rendszer üzemeltetője ISO/IEC27001:2005 információbiztonsági irányítási rendszert alkalmaz, ami érvényes tanúsítvány bemutatása esetén garantálja a rendszer biztonsági osztálya az adminisztratív védelmi intézkedések szempontjából **1,** a rendszer biztonsági osztálya a fizikai védelmi intézkedések szempontjából **2** szintű követelmények teljesülését.

A fentiek alapján állítható, hogy a SIEMENS Zrt. által üzemeltetett számla archiválást végző rendszerelemek 2015.03.11-án vizsgált állapota megfelel a 77/2013. (XII.19.) NFM rendelet 3. és 4. sz. melléklet adminisztratív védelem 1, fizikai védelem 2, logikai védelem [3,3,3] biztonsági osztályába sorolt követelményeinek. A megrendelő által foganatosított adminisztratív, fizikai és logikai védelmi intézkedések garantálják az információbiztonsági veszélyekből származó kockázatok elfogadható mértékű szinten tartását.

Az archiváló rendszer megfelel a digitális archiválás szabályairól szóló 114/2007. (XII. 29.) GKM rendelet 2. §. szerinti követelményének, az 5. § szerinti zárt rendszer alkalmazásával.

3.4 Feltételek

1. A jelen dokumentumban tanúsított kezdeti rendszerértékelés eredményeinek megerősítése, a tanúsítvány érvényességének megtartása és a maradvány kockázatok csökkentése céljából felülvizsgálati rendszerértékelést kell végrehajtani az alábbi esetekben:
   - a tanúsítvány érvényességi időszakában évente egy alkalommal (tervezett felülvizsgálati rendszerértékelés),
   - a rendszer architektúrájában vagy funkcionalitásában bekövetkezett változtatásokra reagálva (rendkívüli felülvizsgálati rendszerértékelés).

   Az első tervezett felülvizsgálati rendszerértékelést tekintettel a kezdeti értékelési jelentésben megállapított kockázatokra legkésőbb **2016. április 15**-ig el kell végezni.

2. A működtetett rendszer architektúrájában vagy funkcionalitásában bekövetkezett jelentős változásokat a Megrendelő köteles a Tanúsítónak a változás érvénybe léptetését követő 30 napon belül bejelenteni, a tanúsítvány kiállítását megelőző vizsgálatoknak megfelelő mélységben a változások leírását tartalmazó dokumentációkat megküldeni.

3. A 2. esetben a tanúsítvány érvényességének fenntartásához a tanúsító értékeli a változásnak a hatásait és dönt a rendkívüli felülvizsgálati rendszerértékelés szükségességéről. A módosított rendszer állapotra – megfelelőség esetén - Tanúsítvány Felülvizsgálati Jegyzőkönyvet állít ki. A tervezett vagy rendkívüli felülvizsgálati rendszerértékelés végrehajtásának feltételeit Megrendelő köteles biztosítani.

4. A Rendszer Biztonsági Előirányzatban megfogalmazott alábbi környezeti biztonsági célokat, a rendszer üzemeltetőjének folyamatosan teljesíteni kell. Ennek igazolására a SIEMENS számla archiváló rendszert tartalmazó területre érvényes ISO/IEC27001:2005 tanúsítvánnyal kell rendelkeznie.

OE.Szervezeti_szintű_alapfeladatok
Az érintett szervezet:
- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonságpolitikát;
- meghatározza az informatikai biztonságpolitika felülvizsgálatának és frissítésének gyakoriságát;
- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági stratégiát, amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését;
- meghatározza az informatikai biztonsági stratégia felülvizsgálatának és frissítésének gyakoriságát;
- gondoskodik arról, hogy az informatikai biztonsági stratégia jogosulatlanok számára ne legyen megismerhető, módosítható.
- megfogalmazza, dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;
- meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;

- gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

Az érintett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg.
Az érintett szervezet:

- elektronikus információs rendszereiről nyilvántartást vezet;
- folyamatosan aktualizálja a nyilvántartást.
- megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;
- felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;
- meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket, kijelöli az ezeket betöltő személyeket;
- integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

OE.Kockázatelemzés

Az érintett szervezet a vizsgált rendszerére vonatkozóan:

- megfogalmazza, dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, kockázatelemzésre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a kockázatelemzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a kockázatelemzési eljárásrendet;
- jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit;
- meghatározza, hogy a rendszerek melyik biztonsági osztályba sorolandók;
- vezetője jóváhagyja a biztonsági osztályba sorolást;
- rögzíti a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában;
- végrehajtja a biztonsági kockázatelemzéseket;
- rögzíti a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy a kockázatelemzési eljárásrendben előírt dokumentumban;
- a kockázatelemzési eljárásrendnek megfelelően felülvizsgálja a kockázatelemzések eredményét;
- a kockázatelemzési eljárásrendnek megfelelően, vagy az informatikai biztonsági szabályzata keretében megismerteti a kockázatelemzés eredményét az érintettekkel;
- amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre;
- gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

OE.Emberi_tényezőket_figyelembe_vevő–személy–biztonság
Az érintett szervezet jogviszony megszűnése esetén:

- belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez;
- megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;
- tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;
- visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;
- megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;
- az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
- a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;
- a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi;
- belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;
- amennyiben az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

OE.Tudatosság_és_képzés
Az érintett szervezet:

- megfogalmazza, dokumentálja, valamint az érintett szervezeten belül kihirdeti az képzési eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, képzésre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;
- a képzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.

Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

- az új felhasználók kezdeti képzésének részeként;
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- az érintett szervezet által meghatározott gyakorisággal.

OE.Fizikai_és_környezeti_védelem
Az érintett szervezet:

- megfogalmazza, dokumentálja, valamint az érintett szervezeten belül kihirdeti a fizikai védelmi eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, fizikai védelme vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

- a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet;
- összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;
- belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;
- rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;
- eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;
- intézkedik a belépési jogosultságot igazoló dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt;
- kizárólag az érintett szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;
- naplózza a fizikai belépéseket;
- ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;
- kíséri a létesítménybe ad-hoc belépésre jogosultakat és figyelemmel követi a tevékenységüket;
- megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;
- nyilvántartást vezet a fizikai belépést ellenőrző eszközről;
- meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;
- az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;
- a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel, vagy eszközzel;
- felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

3.5 Elvárások

A tanúsító elfogadja az értékelők által tett javaslatokat a rendszer vizsgálata során feltárt maradványkockázatok csökkentésére. Elvárja a működtetőtől, hogy az értékelők javaslatait, vagy azokkal egyenértékű egyéb intézkedésekkel a maradványkockázatokat csökkentse. A tervezett felülvizsgálati rendszerértékelés során ezen intézkedések vizsgálata kiemelt szerepet fog kapni.

4 Hivatkozások, rövidítések

4.1 A követelményeket tartalmazó dokumentum

114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól 2. és 5.paragrafusok

4.2 Figyelembe vett jogszabályok, módszertani dokumentumok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (IBTV)

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

MIBÉTS 2009 Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében kidolgozott dokumentum, v4 2008.09.19) (a KIB 28-as számú Ajánlás része)

MIBÉTS 2009 Útmutató rendszer értékelőknek (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében kidolgozott dokumentum, v3 2008.09.19 (a KIB 28-as számú Ajánlás része)

MIBÉTS 2009 IT biztonsági műszaki követelmények a különböző biztonsági szintekre - Követelmény előírás (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében kidolgozott dokumentum, v1.01, 2008.08.22) (a KIB 28-as számú Ajánlás része)

4.3 Rövidítések

MIBÉTS	-	Magyar Informatika Biztonsági Értékelési és Tanúsítási Séma
SAP-F	Security Assurance Package	rendszer garanciacsomag (fokozott)
SETR	System Evaluation Technical Report	rendszer értékelési jelentés
SST	System Security Target	rendszer biztonsági előirányzat
STOE	System Target of Evaluation	a rendszer értékelés tárgya