Ajánlás

Eljárásrendi követelményekre

elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára

Nemzeti Hírközlési Hatóság Hivatala

2008. június

Tartalom

1 Bevezetés

Az elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható működésének kialakítására és a megfelelőség ellenőrzésére két ajánlást jelentő követelményrendszer került kidolgozásra. Jelen dokumentum az archiválási szolgáltatók működésére (eljárásrendjére, szabályzataira) vonatkozik, s összhangban áll a másik követelményrendszerrel, mely a megbízható rendszerek műszaki követelményeit tartalmazza. A két követelményrendszer teljesítésével lehetővé válik az elektronikus aláírásról szóló 2001. évi XXXV. törvény ([eat]) szerinti archiválási szolgáltatók (továbbiakban ASZ) megbízható működésének kialakítása és a megfelelőség ellenőrizhetősége.

A jelen követelményrendszer célközönsége az elektronikus aláírás felhasználásával megvalósított elektronikus archiválási szolgáltatások tervezői, megvalósítói és működtetői, valamint a szolgáltatások megfelelőségének vizsgálatát végző szakértők és a Nemzeti Hírközlési Hatóság (továbbiakban: Hatóság) munkatársai. A tervezők és megvalósítók az eljárásrend és szabályzatrendszer kialakításához kapnak támpontokat. A működtetők az esetlegesen felmerülő bizonytalan kérdésekben találhatnak iránymutatást. A megfelelőség vizsgálatot végző szakértők a jogszabályi követelmények megvalósulását ellenőrizhetik ennek a dokumentumnak az alapján. Ugyanakkor fel kell hívni a figyelmet arra, hogy bár a jelen követelményrendszer a kidolgozásakor hatályban lévő jogszabályokat figyelembe véve készült, azonban egy adott szolgáltatás megfelelőségének megítélésénél a mindenkor hatályos jogszabályi követelményeket, valamint a szolgáltatásra vonatkozó más kötelező előírásokat kell figyelembe venni. A jelen követelményrendszer kötelező erővel nem bír, célja csupán annyi, hogy az irányadó előírások teljesítéséhez segítséget nyújtson. Más, az előírásokat teljesítő megoldások természetesen szintén megfelelőnek minősülnek.

Jelenleg nincs olyan nemzetközileg általánosan elfogadott követelményrendszer, mely jelen dokumentum meghatározó forrása lehetne. Ugyanakkor számos nemzeti és nemzetközi projekt, valamint több szabványosítási tevékenység foglalkozik a kérdéskör különböző aspektusaival. Ezek egy része (rész)eredményekkel lezárult, más része különböző készültségi szinteken álló tervezetek formájában megismerhető.

Jelen követelményrendszer egy részletes témafeldolgozáson alapul, mely hasznosította a nemzetközi tapasztalatokat, egyúttal figyelembe veszi a hazai jogszabályi környezetet is.

A jelen dokumentumban meghatározott szabályozási követelmények az MSZ ISO/IEC 27001:2006 szabványban meghatározott kategóriákon alapulnak.

Az MSZ ISO/IEC 27001:2006 egy információbiztonsági szabályzat szükségességét fogalmazza meg, és célja, hogy egy szervezeten belül világos menedzsmentet és irányítást biztosítson. Jelen dokumentum azokat a követelményeket határozza meg, amelyeket egy archiválási szolgáltatónak érvényre kell juttatnia az információbiztonsági szabályzatán keresztül.

2 Általános fogalmak

2.1 Archiválási szolgáltató

Archiválási szolgáltató az [eat] definíciója szerint olyan szolgáltató, amely az elektronikus aláírással ellátott dokumentumok elektronikus archiválására vonatkozó szolgáltatást nyújtja. A szolgáltató alapvető tevékenységei:

a. letagadhatatlanság biztosítása és a dokumentumok hiteles megőrzése céljából az archiválás időpontjában létező érvényességi lánc archiválása;
b. biztosítja az érvényességi lánc sértetlenségét az ahhoz tartozó elektronikus aláírások érvényességének hosszú távú ellenőrizhetősége érdekében;
c. az érvényességi láncot az igénybe vevő kérésére annak haladéktalanul átadja;
d. kérelemre igazolást bocsát ki az általa archivált elektronikus dokumentummal vagy érvényességi lánccal kapcsolatban.

Az érvényességi lánc tekintetében az [eat] definíciója a mérvadó.

2.2 Archiválási szolgáltatások

2.2.1 Funkciók csoportosítása

Egy archiválási szolgáltatónak (s így megbízható rendszerének is) a következő funkciókat (funkciócsoportokat) kell biztosítania. Az egyes funkciók felsorolásánál feltüntetésre került, hogy azokat minden archiválás szolgáltatónak biztosítja-e (*kötelező*), vagy az adott funkció biztosítása a szolgáltató vállalásától, illetve az előfizetővel kötött megállapodásától függ (*választható*):

- Befogadással kapcsolatos funkciók (Befogadás funkciócsoport)
- Megőrzéssel kapcsolatos funkciók (Megőrzés funkciócsoport)
- Kibocsátással kapcsolatos funkciók (Kibocsátás funkciócsoport)

Befogadás funkciócsoport: Az archiválási szolgáltató benyújtók számára biztosított közvetlen funkciói a benyújtott információk befogadásával kapcsolatosan. A befogadás funkciócsoport funkciói az alábbiak:

- A benyújtó azonosítása és jogosultságának ellenőrzése – *kötelező*
- Az archiválásra benyújtott adat fogadása – *kötelező*
- Az archiválásra benyújtott információk (köztük az elektronikus aláírás) ellenőrzése – *kötelező*
- A megőrzési időtartam kezelése, befejezése – *kötelező*
- Az archiválással kapcsolatosan benyújtott információk visszaigazolása – *kötelező*
- A hozzáférési jogosultságok kezelése – *kötelező*

Megőrzés funkciócsoport: Az archiválási szolgáltató lényegi funkciói a befogadott információk folyamatos védelmére és megőrzésére. A megőrzés funkciócsoport funkciói az alábbiak:

- Az archivált elektronikus adatok rendelkezésre állásának a megőrzése – *kötelező*
- Az archivált elektronikus adatok sértetlenségének megőrzése – *kötelező*
- Az archivált elektronikus adatok bizalmasságának megőrzése – *kötelező*
- Az archivált elektronikus adatok titkosított formában történő megőrzése – *választható*
- Az archivált elektronikus adatok hitelességének és letagadhatatlanságának megőrzése – *kötelező*

- Az archivált elektronikus adatok olvashatóságának és értelmezhetőségének a fenntartása – *választható*
- Az archivált információk törlése az archiválásra vonatkozó szolgáltatási szerződés szerinti esetekben – *kötelező*

Kibocsátás funkciócsoport: Az archiválási szolgáltató hozzáférők számára biztosított közvetlen funkciói az archivált adatokhoz való hozzáférés biztosítására és ennek ellenőrzésére.

A kibocsátás funkciócsoport funkciói az alábbiak:

- A hozzáférő azonosítása és hitelesítése – *kötelező*
- Az archivált adat kiadása a jogosult hozzáférőnek (Adatkérés teljesítése) – *kötelező*
- Igazolások kiadása az archivált adatokra (Igazolás kérések teljesítése) – *kötelező*
- Az archivált adat és igazolás átadása más archiválási szolgáltatónak (A szolgáltatás befejezés előkészítése) – *kötelező*

2.2.2 Az archiválandó adatok csoportosítása

A benyújtó különböző tartalmú és formátumú adatot nyújthat be archiválásra, melyek érintik az igénybe vehető szolgáltatások körét. Az alábbi három csoport különböztethető meg:

- **Bitfolyam:** az archiválási szolgáltató számára értelmezhetetlen bitsorozat. Bitfolyamra példák: titkosított, tömörített állományok, illetve a szolgáltató által (értelmezhetőség szempontjából) nem támogatott formátumú állományok.
- **Lenyomat:** olyan speciális bitfolyam, amely az archiválási szabályzatban meghatározott lenyomatoló algoritmus felhasználásával egy dokumentumból készült. Lenyomatra példa egy tetszőleges állományból származó, SHA-512 lenyomatoló (hash) függvénnyel készített 64 bájt.
- **Dokumentum:** olyan speciális bitfolyam, amelynek a formátuma megfelel azon dokumentum formátumok egyikének, aminek az értelmezhetőségét az archiválási szolgáltató (kiegészítő szolgáltatásként) vállalja. Dokumentumra példák: rtf, txt, xml formátumú állományok.

Az archiválandó adatoknak a benyújtáskor egy vagy több fokozott biztonságú, vagy minősített elektronikus aláírással kell ellátva lenniük.

2.2.3 Az archiválási szolgáltatás igénybevevői

Előfizető
Az a természetes vagy jogi személy, aki archiválási szerződést köt a szolgáltatóval és az archiválásra átadott adatok tulajdonosa.

Adatgazda, benyújtó
Az előfizető által meghatározott szerepkört betöltő természetes személy, aki

a. az archiválási szolgáltatónak adatot archiválásra benyújt,
b. az általa benyújtott adat tekintetében
   - archiválási időt változtat,
   - teljes jogú hozzáférő
   - további hozzáférő számára jogosultságot ad.

Hozzáférő
Az adatgazda (benyújtó) rendelkezése szerint archivált adatot kikér, igazolást kér, vagy egyéb meghatározott tevékenységet végeztet.

2.2.4 Archiválási szolgáltatások csoportosítása

Egy archiválási szolgáltatónak (s így megbízható rendszerének is) a következő **kötelező (alap) szolgáltatások**at kell biztosítania, az archiválás időtartama alatt:

- **Az archivált adat rendelkezésre állásának biztosítása (rendelkezésre állás):** Ez a szolgáltatás azt garantálja, hogy az archivált adatokat a szolgáltató (az archiválás időtartamának végéig) megőrzi, s az erre jogosult hozzáférők számára (folyamatosan) elérhetővé teszi.
- **Az archivált adat sértetlenségének biztosítása (sértetlenség):** Ez a szolgáltatás azt garantálja, hogy az archivált adatokat a szolgáltató oly módon őrzi meg, amely megakadályozza azok módosítását és jogosulatlan megsemmisítését.
- **Az archivált adat bizalmasságának biztosítása (bizalmasság):** Ez a szolgáltatás azt garantálja, hogy az archivált adatokat a szolgáltató oly módon őrzi meg, amely megakadályozza azok szolgáltatón keresztüli jogosulatlan megismerését az archiválás időtartama alatt.
- **Az archivált adat eredet hitelességének és tartalom letagadhatatlanságának a biztosítása (letagadhatatlanság):** Ez a szolgáltatás azt garantálja, hogy az – archivált adatot a benyújtás előtt elektronikus aláírással ellátó – aláíró utólag nem vitathatja, hogy az adat tőle származik.
- **Az archivált adat törlése (törlés):** A szolgáltató biztosítja, hogy az archivált adatot az arra jogosult megfelelően hitelesített kérése alapján, továbbá az archiválás befejezésekor a rendszeréből visszaállíthatatlanul törli.
- **Igazolások kiadása:** Ez a szolgáltatás azt garantálja, hogy az archivált adatokkal kapcsolatos különböző tényekről a szolgáltató a hozzáférők számára hiteles igazolásokat képes kibocsátani.

Egy archiválási szolgáltató (s így megbízható rendszere is) a következő **választható (kiegészítő) szolgáltatások**at biztosíthatja, az archiválás időtartama alatt:

- **Az archivált adat értelmezhetőségének biztosítása (értelmezhetőség):** Ez a szolgáltatás az archivált adat eredeti céljának folyamatos megvalósíthatóságát garantálja (pl. kép és szöveg esetén megjeleníthetőséget).
- **Az archivált adat titkosított formában való tárolása a szolgáltatónál (titkosítás):** A szolgáltató vállalhatja, hogy a hozzá részben vagy egészben titkosítatlanul benyújtott archivált adatokat a befogadás után titkosítja és ilyen módon tárolja a bizalmasság fokozott biztosítása érdekében.

Egy archiválási szolgáltató (s így megbízható rendszere is) egyéb szolgáltatásokat is biztosíthat (pl. az archivált adatok egyedi megállapodás szerinti feldolgozását). Jelen dokumentum ezekre nézve nem fogalmaz meg kötelező elvárásokat, azon túl, hogy ezek az egyéb szolgáltatások nem akadályozhatják meg a kötelező követelmények teljesülését.

A kiegészítő szolgáltatások igénybevételéről az archiválandó adat beadásakor az adatgazdának nyilatkoznia kell.

2.3 Archiválási szolgáltatási szintek

Jelenleg a törvényi szabályozás minősített és nem minősített archiválás szolgáltatást különböztet meg. Alapvető különbség, hogy az [eat] csak minősített archiválás szolgáltatás igénybevételénél ad az igénybevevő számára kedvező vélelmet egy későbbi bizonyításnál. Nem minősített szolgáltatás esetén semmiféle vélelem nincs.
Jelen követelményrendszerben [minősített] vagy [nem minősített] jelölés alkalmazásával mutatjuk, amennyiben a két szolgáltatási szintre eltérő követelmény került megfogalmazásra.

3 Kötelezettségek és felelősségek

3.1 A megbízható szolgáltatók kötelezettségei

a. Az ASZ-nek garantálnia kell, hogy a 4. és 5. fejezetben részletezetteknek megfelelően minden követelménynek megfelel a nyújtott szolgáltatások tekintetében.
b. Az ASZ felelősséggel tartozik a szabályzataiban előírt eljárások betartásáért, még akkor is, ha folyamatainak egy részét, vagy egészét alvállalkozókra bízza.
c. Az ASZ-nek a felkínált bizalmi szolgáltatásokat az érvényben lévő szolgáltatási szerződésekkel, saját szolgáltatási szabályzatával összhangban és a vonatkozó törvények és szabályozások betartása mellett kell biztosítania.
d. Az ASZ-nek megfelelő pénzügyi garanciát kell biztosítania a szolgáltatás során esetlegesen okozott károk, a tevékenység befejezésével kapcsolatos költségek, valamint a hatósági büntetések fedezetéül.

3.2 Az előfizető kötelezettségei

Az ASZ-nek szerződésen keresztül köteleznie kell az előfizetőt arra, hogy figyelembe vegye a következő kötelezettségeket. Ha a szolgáltatás használója (benyújtó, hozzáférő) és az előfizető különböző entitások, akkor az előfizetőnek tudatosítania kell a szolgáltatás használójával, hogy ezen kötelezettségek a szolgáltatás használójára is vonatkoznak.

a. Csak olyan elektronikus aláírás formátumban küldjön dokumentumokat az ASZ számára, amely megfelel a szerződésben megadott követelményeknek.
b. Garantálnia kell az ASZ szolgáltatások használatával kapcsolatos minden kulcs, biztonsági eszköz, jelszó és biztonsági token biztonságát, és ezeket csak az előfizetői tájékoztatásban közölt minden egyéb korlátozással összhangban szabad használnia.
c. Az ASZ dokumentumtárolóhoz való hozzáféréskor alkalmaznia kell a biztonsági intézkedéseket az ASZ által előírt módon.
d. Meg kell tennie minden olyan óvintézkedést, amelyet szerződésekben vagy másutt előírtak.

3.3 Felelősség

Az ASZ az érvényességi lánc vagy az általa őrzött elektronikus dokumentumok, illetve lenyomatok sérülése vagy megsemmisülése miatt más személynek okozott kárt köteles megtéríteni. A szolgáltató mentesül a felelősség alól, ha bizonyítja, hogy a kárt tevékenységi körén kívül eső elháríthatatlan ok idézte elő.

a. A szolgáltató a szolgáltatási szabályzatban az érvényességi lánc vagy az általa őrzött elektronikus dokumentumok, illetve lenyomatok sérülése vagy megsemmisülése által más személynek okozott kár tekintetében felelősségét korlátozhatja.

4 Archiválási szolgáltatásra vonatkozó követelmények

Az ASZ-nek olyan ellenőrzéseket kell megvalósítania, amelyek kielégítik a következő követelményeket.

4.1 Szolgáltatási és archiválási szabályzat

Követelmény: Az ASZ-nek rendelkeznie kell szolgáltatási szabályzattal, és ennek részeként archiválási szabályzattal, amely e dokumentumban meghatározott összes követelményre kiterjed, illetőleg tartalmazza az alábbiakat:

a. a szolgáltató székhelyének, telephelyének postacímét és telefonszámát, illetve a szolgáltató elérhetőségének egyéb távközlési azonosítóját;
b. a szolgáltató cégjegyzékszámát, illetve a szolgáltató egyéni vállalkozó vállalkozói igazolványának számát;
c. a szolgáltató nem minősített szolgáltatóként, illetve minősített szolgáltatóként való nyilvántartásba vételének napját a Hatóság erről szóló határozata szerint, e határozat közlése előtt a nyilvántartásba vétel meg nem történtének feltüntetését;
d. a szolgáltatási szabályzat változatának azonosítóját (verziószámát);
e. a szolgáltatási szabályzat hatálybalépését és hatályának a megszűnését;
f. a szolgáltató által a szolgáltatás nyújtásához használt elektronikus aláírási termékek megnevezését (intelligens kártya, HSM modul, aláírás-létrehozó és ellenőrző alkalmazás), valamint a szolgáltató nyilatkozatát arról, hogy ezek az elektronikus aláírási termékek rendelkeznek a jogszabályok szerinti megfelelőségi igazolással;
g. utalást arra, hogy a szolgáltató önkéntes akkreditációs rendszer keretében tanúsítva lett-e;
h. a szolgáltató tevékenységével kapcsolatos kifogások és panaszok bejelentésének helyét és módját, a szolgáltatói ügyfélszolgálat és az illetékes fogyasztóvédelmi felügyelőség elérhetőségét;
i. a szolgáltató által vállalt egyes nyitvatartási és rendelkezésre állási időket;
j. tájékoztatást a szolgáltató által nyújtott szolgáltatásokról és azok felhasználásának módjáról;
k. adatkezelési szabályzatot, amely összefoglaló jellegű tájékoztatást ad a szolgáltató által kezelt adatok fajtájáról, az adatkezelés céljáról, a továbbított adatok fajtájáról, címzettjéről, az adattovábbítás jogalapjáról, valamint az egyes adatfajták törlési határidejéről.
l. Az ASZ kizárólag elektronikus dokumentumok (mint tartalom információ) és az ehhez tartozó elektronikus aláírások (mint a megőrzés leíró információ egyik eleme) együttes megőrzését vállalja, vagy a benyújtó által őrzött tartalom információkhoz tartozó különálló, a dokumentum lenyomatán elhelyezett elektronikus aláírások archiválását is,
m. a támogatott aláírás formátumokat és azok kezelését, a támogatott kriptográfiai aláírás-készletet (hash függvény, feltöltési eljárás és aláíró algoritmus a paramétereivel),
n. azon hitelesítési rendeket, amelyek szerint kibocsátott tanúsítványokat az archiválás szolgáltató a benyújtott dokumentumokon szereplő elektronikus aláírások ellenőrzésére elfogadja, megjelölve az adott hitelesítési rendeket alkalmazó hitelesítés-szolgáltatókat is. A szabályzatnak tartalmaznia kell azt is, hogy a tanúsítványok és az aláírások ellenőrzésére az archiválás szolgáltató milyen visszavonási információ szolgáltatásokat támogat (CRL és/vagy OCSP),

o. azon időbélyegzési rendeket, amelyek szerint kibocsátott időbélyegeket az archiválás szolgáltató az archiválásra benyújtott dokumentumokon elfogad, megjelölve az adott időbélyegzési rendeket alkalmazó időbélyeg-szolgáltatókat is,
p. a benyújtott elektronikus dokumentumok (mint tartalom információ) értelmezhetőség szempontjából támogatott formátumait,
q. az archiválási szolgáltató és a benyújtó közötti adatcseréhez használható protokollokat,
r. az archivált dokumentumok egyedi azonosítására alkalmazandó mechanizmust.
s. az archiválási szolgáltató és a felhasználó közötti adatcseréhez használható protokollokat.

[Minősített]

a. az előfizetővel való együttműködés szabályait abban az esetben, ha a szolgáltató által megőrzött érvényességi láncnak az elektronikus dokumentum nem része, így különösen azon időtartam és események meghatározását, amely eltelte vagy amelyek beállta esetén az előfizető köteles az elektronikus dokumentumnak a Hatóság által meghatározott elfogadott kriptográfiai algoritmus alkalmazásával képzett lenyomatát az archiválási szolgáltató számára átadni;
b. archiválási szabályzatot, amely tartalmazza azon dokumentumformátumok felsorolását, amelyek vonatkozásában az archiválási szolgáltató vállalja a értelmezhetőség (olvashatóság) és megjeleníthetőség folyamatos fenntartását, az értelmezhetőség és megjeleníthetőség biztosítását szolgáló eljárásrendet, ideértve a hardver- és szoftvereszközök rendelkezésre állásának biztosítására (emuláció) vonatkozó szabályokat, illetve az új adathordozóra vagy új formátumba történő átvitellel (migráció) kapcsolatos eljárásrendet is, valamint az ezen dokumentumformátumokban őrzött dokumentumokkal kapcsolatban a szolgáltató működésének befejezése esetén követendő eljárást;
c. a kárviselés szabályait és a felelősségkorlátozást;
d. részletes adatkezelési szabályzatot, amely szabályozza a szolgáltató minden személyes adatkezelését, rögzíti azok célját, jogalapját és a törlési határidőket, a megkeresésekről szóló nyilvántartás vezetését, a megkeresések teljesítésekor követendő eljárást;
e. az igazolások kiadása során követett eljárást;
f. annak a leírását, hogy a szolgáltató miként biztosítja a szolgáltatási szabályzatban előírt folyamatos rendelkezésre állást;
g. annak a leírását, hogy a szolgáltató
   – milyen módon felel meg az üzemeltetési és hozzáférési biztonsági követelményeknek,
   – milyen termékeket használ a szolgáltatás nyújtásához, illetve ahhoz, hogy az üzemeltetési és hozzáférési biztonsági követelményeknek megfeleljen,
   – miként kívánja az üzemeltetés során előforduló hibákat, így különösen a karbantartási és telepítési hibákat elkerülni,
   – az üzemeltetés ellenőrzéséhez milyen eljárásokat alkalmaz;
h. annak a leírását, hogy az informatikai rendszer felhasználóinak milyen hozzáférési jogosultsággal kell rendelkezniük ahhoz, hogy az informatikai rendszerben bizonyos tevékenységeket elvégezhessenek;
i. a rendkívüli üzemeltetési helyzet esetén követendő eljárás leírását;
j. a bizalmi munkakörök nevesítését és leírását;
k. a benyújtó azonosítására szolgáló eljárást.

4.2 Tájékoztatás

Követelmény: A szolgáltatónak a szerződéskötést megelőzően tájékoztatnia kell az előfizetőt a szolgáltatás felhasználásának módjáról, biztonsági fokáról, szolgáltatási szabályzatáról, a szerződés feltételeiről, valamint az alkalmazandó adatvédelmi szabályokról.

l. Tájékoztatást kell adni azon dokumentumformátumokról, amelyek vonatkozásában az archiválási szolgáltató vállalja az értelmezhetőség (olvashatóság) folyamatos fenntartását a szolgáltatási szabályzat szerint.
m. Tájékoztatást kell adni az előfizető azon kötelezettségéről, amely szerint, ha az érvényességi lánc nem tartalmazza az elektronikus dokumentumot, a szolgáltatási szerződésben meghatározott időközönként és esetekben köteles az elektronikus dokumentumnak a Hatóság által közzétett elfogadott kriptográfiai algoritmus alkalmazásával képzett lenyomatát a szolgáltató számára fokozott biztonságú vagy minősített elektronikus aláírásba foglalva átadni, valamint tájékoztatni kell e kötelezettség elmulasztásának következményeiről.
n. Tájékoztatást kell adni az elektronikus aláírások hosszú távú érvényesítéséhez szükséges információk köréről, valamint annak következményeiről, ha az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információk nem szerezhetők be.
o. Tájékoztatást kell adni az archiválási szolgáltató személyes adatkezeléséről, így különösen a harmadik személyek számára külön törvény által biztosított hozzáférés lehetőségéről, a megkeresésekkel kapcsolatos nyilvántartás vezetéséről és a hozzáférés feltételeiről, a szerződés teljesítéséhez szükséges adatok kezeléséről, valamint – amennyiben az az előfizető vagy megbízottja személyes adatainak kezelésével jár – a naplózás során történő személyes adatok kezeléséről.
p. Tájékoztatást kell adni az archiválási szolgáltató esetleges felelősségkorlátozásáról.
q. Tájékoztatást kell adni az archiválási idő leteltét követő eljárásrendről és az esetleges szerződésszegés jogkövetkezményeiről.
r. Az ASZ-nek információbiztonsági esemény bekövetkeztekor az érintett adatok tulajdonosait teljes körűen tájékoztatni kell az esemény bekövetkezéséről és hatásairól.

4.3 Szolgáltatási követelmények

4.3.1 Kötelező szolgáltatások

Az alábbi követelmények minden archiválási szolgáltatóra érvényesek.

4.3.1.1 Rendelkezésre állás biztosítása

Követelmény: Az ASZ-nek elérhetővé kell tennie a dokumentumokat a feljogosított felek számára az alkalmazott jogszabályoknak és szabályzatoknak, valamint az előfizetővel kötött szerződésnek megfelelően.

a. Hozzáférést kell adni az előfizetőnek, az adatgazdának valamint a hozzáférőnek (a dokumentum tulajdonosainak), és a törvény által feljogosított hatóságoknak.
b. Az archivált adatot védeni kell a jogosulatlan törlés vagy megsemmisítés ellen.

Követelmény: Az ASZ-nek biztosítania kell, hogy az adatgazda meghatározhassa az archiválási időtartamot.

a. Biztosítani kell az archiválási időtartam megváltoztatásának lehetőségét.

b. Biztosítani kell az archivált adatra vonatkozó teljes érvényességi lánc adatgazda által meghatározottaknak történő átadását.

4.3.1.2 Sértetlenség biztosítása

Követelmény: Az ASZ-nek biztosítania kell az archivált adat sértetlenségének megtartását a tárolás teljes időtartama alatt.

a. Az archivált adatot védeni kell módosítás ellen.

Követelmény: Az ASZ-nek biztosítania kell, hogy a dokumentumokat tároló adathordozó az idővel szemben ellenáll, illetve működtethetősége garantált.

a. Amennyiben lehetséges, olyan adathordozót és olvasót kell alkalmazni, amely a megkövetelt teljes tárolási időtartamban garantáltan ellenáll az időnek. Amennyiben műszaki elöregedés vagy fizikai kopás miatt fennáll a kockázata annak, hogy az adathordozó olvashatatlanná válik, akkor az olvashatóság fenntartása érdekében a tartalmat megfelelő időközönként másik megfelelő adathordozóra kell másolni.

4.3.1.3 Létezés bizonyítása

Követelmény: Az ASZ-nek hitelt érdemlő módon kell bizonyítania az archivált adat egy adott időpont utáni létezését, illetve a beadás időpontjának tényét.

a. A létezés bizonyításához minősített hitelesítés szolgáltató által kiadott időbélyeget kell elhelyezni az archivált adaton.
b. Az időbélyegen lévő elektronikus aláírás érvényességét fenn kell tartani az archiválás teljes időtartama alatt.

4.3.1.4 Bizalmasság biztosítása

Követelmény: Az ASZ-nek biztosítania kell a különböző adatgazdák által archiválásra átadott adatok bizalmasságát.

a. A tárolás során a különböző tulajdonosú adatoknak fizikailag vagy logikailag el kell különülniük egymástól a bizalmasság fenntartása érdekében.
b. Az elektronikus dokumentumok tartalmát az ASZ, vagy vele megbízási vagy munkaviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban álló személyek csak az adatgazda írásbeli engedélyével ismerhetik meg.
c. Az archivált adatot védeni kell jogosulatlan hozzáférés ellen.
d. Amennyiben az ASZ távoli hozzáférést biztosít a dokumentumokhoz, azt oly módon kell megvalósítani, hogy a sértetlenség és a bizalmasság nem megbízható hálózat alkalmazása esetén is fennmaradjon.

4.3.1.5 Hitelesség és letagadhatatlanság biztosítása

Követelmény: Az ASZ-nek biztosítania kell az eredet hitelességének megőrzését, és a felelősségvállalás érvényességének (letagadhatatlanságának) fenntartását az elektronikusan aláírt adatok tartalmára vonatkozóan a tárolás teljes időtartama alatt.

a. A szolgáltatás csak olyan adat tekintetében nyújtható, amit az adatgazda (benyújtó) legalább egy fokozott biztonságú vagy minősített elektronikus aláírással látott el.
b. Az elektronikus aláírás érvényessége ellenőrizhetőségének fenn kell maradnia a tárolás teljes időtartama alatt.
c. Ha az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információk nem szerezhetők be, vagy az elektronikus aláírás ellenőrzése érvénytelen eredményt ad, az ASZ köteles erről a tényről az igénybe vevőt haladéktalanul tájékoztatni, illetve a szolgáltatás nyújtását el kell utasítania.

d. Lenyomat formátumú adat esetén csak az alkalmazott lenyomat (hash) algoritmus meggyengüléséig biztosítható a szolgáltatás.

4.3.1.6 Archivált adatok törlése:

Követelmény: Az ASZ-nek biztosítania kell, hogy az arra jogosult fél megfelelően hitelesített kérésére az érvényességi láncot a rendszeréből visszavonhatatlanul törölje.

a. A szolgáltatási szerződés megszűnése vagy az adatgazda ilyen rendelkezése esetén az archiválási szolgáltató köteles az érvényességi láncot visszaállíthatatlan módon törölni informatikai rendszeréből.

Az ASZ-nek eljárásokat kell meghatároznia az archiválási időtartam eltelte után foganatosítandó intézkedésekről.

4.3.1.7 Igazolások kiadása

Követelmény: Az ASZ-nek igazolásokat kell kiadnia a feljogosított felek számára az alkalmazott jogszabályoknak, szabályzatoknak és az előfizetőkkel kötött szerződéseknek megfelelően.

a. Ha az ASZ az igazolást elektronikus úton állítja ki, úgy az elektronikus dokumentumon minősített elektronikus aláírást kell elhelyeznie, valamint minősített szolgáltató által kibocsátott időbélyegzőt elhelyeznie vagy elhelyeztetnie az Informatikai és Hírközlési Minisztérium által kidolgozott, a közigazgatásban alkalmazható elektronikus aláírás formátumokra vonatkozó műszaki specifikációban meghatározott elektronikus aláírás formátumban.
b. Az igazolást harmadik személy számára is ki kell adni, amennyiben a kérelméhez csatolja az adatgazda teljes bizonyító erejű magánokiratba foglalt meghatalmazását.

4.3.2 Kiegészítő szolgáltatások

Az alábbi követelmények csak abban az esetben értelmezhetőek az archiválási szolgáltatóra, amennyiben vállalja a kiegészítő szolgáltatás nyújtását, valamint az archiválandó adat tekintetében a beadó igényli.

4.3.2.1 Az archivált adat titkosított formában való tárolásának biztosítása (titkosítás)

Követelmény: A szolgáltató biztosítja, hogy a hozzá részben vagy egészben titkosítatlanul benyújtott archivált adatokat a befogadás után titkosítja és ilyen módon tárolja a bizalmasság érdekében.

a. A szolgáltató köteles biztosítani megfelelő kriptográfiai mechanizmusokat, azaz megfelelő (megbízható és helyesen megvalósított) titkosító algoritmust, megfelelő kulcsméretet, biztonságos kulcselőállítási módszert és kulcskezelési eljárásokat köteles alkalmazni a szolgáltatás nyújtása során.
b. A szolgáltatás csak lenyomat benyújtása esetében nem értelmezhető.

4.3.2.2 Értelmezhetőség biztosítása

Követelmény: Az ASZ-nek a szolgáltatási szabályzatban fel kell tüntetnie, hogy mely dokumentum formátumok folyamatos értelmezhetőségének a biztosítását vállalja.

a. Valamennyi meghatározott dokumentum formátumra az értelmezhetőséghez szükséges környezetet (hardver, platform, megjelenítő alkalmazás) a tárolás teljes időtartama alatt biztosítani kell.
b. Egyértelműen jelezni kell, ha az értelmezésre kerülő dokumentum olyan rejtett vagy aktív kódot tartalmaz, ami a dokumentum megjelenítésében változást okozhat.

c. Az ASZ-nek az értelmezhetőség biztosítására átadott dokumentum formátumát meg kell határoznia, és amennyiben a formátumot nem támogatja, el kell utasítani az értelmezhetőség, vállalását.
d. A szolgáltatási szabályzatban meghatározott elektronikus aláírás formátumok értelmezhetőségét Az ASZ-nek biztosítania kell.

4.3.2.3 Egyéb szolgáltatás

Követelmény: Az ASZ csak olyan egyéb szolgáltatást vállalhat, amely nem sérti a kötelező szolgáltatások biztonságát.

a. Egyéb szolgáltatás nyújtása során az archivált adatok bizalmasságát, sértetlenségét és rendelkezésre állását meg kell őrizni.

4.4 Legalább fokozott biztonságú elektronikus aláírás kezelése

Követelmény: Az ASZ-nek biztosítania kell az archivált adaton elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás(ok) érvényességének ellenőrizhetőségét a letagadhatatlanság megőrzésének teljes időtartama alatt.

a. Az elektronikus aláírás érvényességének megállapításához szükséges összes információt (tanúsítványok, a végtanúsítványra vonatkozó visszavonási információ) illetőleg az elektronikus aláírás adott időbeni létezését megbízható módon jelző adatot (időbélyeg) a befogadástól számított három napon belül be kell szerezni.
b. Amennyiben létezik megbízható információ azon időpontról, amikor az elektronikus aláírás már létezett, akkor ezt kell az ellenőrzés alapjául tekinteni.
c. Az érvényesítő adatokat az archivált adattal logikailag összekötve kell tárolni.
d. Az elektronikus aláírás ellenőrzést a CEN CWA 14171:2004 dokumentumban meghatározott módon kell elvégezni.
e. A nem végtanúsítványra vonatkozó új visszavonási információk meglétét naponta ellenőrizni kell, a megjelenő új információt pedig archiválni kell.
f. Az archiválandó dokumentum beadásakor, illetve amennyiben a tárolási idő hosszabb, mint az alkalmazott kriptográfiai algoritmusok erősségének érvényességi ideje, valamint hatósági határozatra kiegészítő eljárásokat kell alkalmazni az elektronikus aláírás hitelességének biztosítása érdekében. A kiegészítő eljárások alkalmazásának időpontját, hitelt érdemlő módon az archiválás teljes időtartama alatt bizonyítani kell.

4.5 Az ASZ működésének megszűnése

Követelmény: A szolgáltatónak működésének befejezése esetén az érvényességi láncot a hitelesség ellenőrizhetőségének megtartása mellett az adatgazdának/előfizetőnek, illetve más, vele azonos szintű szolgáltatást nyújtó archiválás szolgáltatónak át kell adnia.

a. Az ASZ megfelelő időben (legalább 60 nap) tájékoztatni köteles a megszüntetésről a Hatóságot, valamint az összes olyan dokumentum tulajdonost és egyéb entitásokat, amelyekkel Az ASZ-nek szerződése vagy más formájú, megalapozott kapcsolata van.

5 Az információbiztonság irányítására vonatkozó követelmények

[Minősített]
Az ASZ-nek igazolnia kell, hogy Információ biztonság kezelő rendszere (ISMS Information Security Management System) valamely általánosan elismert szabványnak megfelel. (Ilyen szabvány például az MSZ ISO/IEC 27001:2006) .

[Nem minősített]
Javasolt, hogy az ASZ rendelkezzen valamely általánosan elismert információbiztonsági irányítási rendszerrel (pl: MSZ ISO/IEC 27001:2006 vagy hasonló)

5.1 Kockázatelemzés

Az ASZ-nak rendszeres időszakonként kockázatelemzést kell végeznie, hogy azonosítsa, számszerűsítse és szervezeti célok és kockázatelfogadási kritériumok alapján sorolja be a releváns kockázatokat.

a. A szolgáltatások nyújtásához használt valamennyi elektronikus aláírási terméket a kockázatelemzés alapján biztonsági osztályokba kell sorolni, és ezekről nyilvántartást kell vezetni.

5.2 Az információbiztonsági szabályzat

Követelmény: Az ASZ vezetésének iránymutatást és támogatást kell nyújtania az információbiztonság, a működés követelményeinek, valamint a vonatkozó törvényeknek és szabályozásnak megfelelően.

a. Érvényben kell lennie egy információbiztonsági szabályzatnak, és az ASZ-nek érvényre kell juttatnia ennek ismeretét és betartását.

5.3 Az információbiztonság szervezete

5.3.1 Belső szervezet

Követelmény: Az ASZ-nek irányítási keretrendszert kell létrehoznia, hogy kialakítsa és szabályozza az információbiztonság bevezetését a szervezeten belül.

a. Az MSZ ISO/IEC 17799:2006 6.1-es pontja szerinti intézkedéseket ajánlott alkalmazni.

5.3.2 Külső felek

Követelmény: Az ASZ-nek fenn kell tartania a szervezet információbiztonságát és azon információfeldolgozó eszközeinek biztonságát, amelyekhez külső felek hozzáférnek, amelyeken az információ feldolgozása, közlése történik a külső felek felé, vagy amelyeket azok kezelnek.

a. Megfelelő szerződési kitételeket szükséges érvényesíteni az ASZ és az alvállalkozónak bevont szervezet között, ami egyértelműen meghatározza az alvállalkozó kötelességeit és felelősségeit, lefedve az általános szabályok által nem kezelt részleteket is.
b. Az MSZ ISO/IEC 17799:2006 6.2-es pontja szerinti intézkedéseket ajánlott alkalmazni.

5.4 Vagyontárgyak kezelése

5.4.1 Felelősség a vagyontárgyakért

Követelmény: Az ASZ-nek ki kell alakítania, és fenn kell tartania a vagyontárgyai megfelelő védelmét.

a. Az MSZ ISO/IEC 17799:2006 7.1-es pontja szerinti intézkedéseket ajánlott alkalmazni.

5.4.2 Információosztályozás

Követelmény: Az ASZ-nek biztosítania kell az információk megfelelő szintű védelemét.

a. Minden magán aláíró kulcsot érzékeny adatként kell kezelni, és speciális intézkedésekkel kell védeni.
b. Minden archiválásra átadott dokumentumot az ASZ bizalmas dokumentumaként kell kezelni, és mint ilyet, csak az adatgazda által adott feljogosításnak megfelelően lehet felfedni más személyek számára.
c. Az ASZ-nek leltárt kell vezetnie összes információs vagyontárgyáról, és a kockázatelemzéssel összhangban osztályoznia kell azokat a védelmi követelmények szerint.
d. Az MSZ ISO/IEC 17799:2006 7.2-es pontja szerinti intézkedéseket ajánlott alkalmazni.

5.5 Az emberi erőforrások biztonsága

5.5.1 Az alkalmazás előtt

Követelmény: Az ASZ-nek biztosítania kell, hogy az alkalmazottak, alvállalkozók és harmadik fél felhasználók megértették a kötelezettségeiket, és alkalmasak arra a szerepkörre, amelyre kiválasztották őket, így csökkentve a lopás, csalás vagy a lehetőségekkel való visszaélés kockázatát.

a. Bizalmi munkakör várományosával minden esetben világosan, írásban kell ismertetni a feladatait és felelősségeit, és ezeket neki írásban kell elfogadnia.
b. Az ASZ munkatársait a bizalmi munkakörökbe a szolgáltató informatikai rendszeréért általánosan felelős vezetőnek kell hivatalosan kineveznie.
c. Az ASZ-nek nem szabad bizalmi szerepkörbe vagy vezetői munkakörbe kineveznie olyan személyt, akiről ismert, hogy súlyos bűncselekmények, vagy olyan egyéb cselekmények miatt ítélték el, amely befolyásolja az e munkakörre való alkalmasságát.
d. A munkatársaknak mindaddig nem szabad hozzáférniük a bizalmi funkciókhoz, amíg a szükséges ellenőrzések le nem zárultak.
e. Az MSZ ISO/IEC 17799:2006 8.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.5.2 Az alkalmazás alatt

Követelmény: Az ASZ-nek biztosítania kell, hogy az alkalmazottak, alvállalkozók és harmadik fél felhasználók tisztában vannak az információbiztonsági veszélyekkel és problémákkal, a felelősségeikkel és kötelezettségeikkel, továbbá megfelelő felszerelésekkel és ismeretekkel rendelkeznek ahhoz, hogy mindennapi munkájuk folyamán megfeleljenek a szervezeti biztonsági szabályzatoknak, és hozzájáruljanak az emberi hibák kockázatának csökkentéséhez.

a. A vonatkozó törvényekkel és jogszabályokkal összhangban, a bizalmi munkakört betöltő személyzetet, beleértve az érintett vezetőket, megfelelően el kell látni a szükséges ismeretekkel és felszereléssel, hogy helyesen és biztonságosan végezzék a munkájukat, és megfelelően és kellő időben ki kell képezni őket a munkaköri

feladataikra, és ismertetni kell velük a lehetséges helytelen cselekedeteik következményeit.

b. Az MSZ ISO/IEC 17799:2006 8.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.5.3 Az alkalmazás megszűnése vagy változása

Követelmény: Az ASZ-nek biztosítania kell, hogy az alkalmazottak, alvállalkozók és harmadik fél felhasználók rendezett módon hagyják el a szervezetet, vagy változtassanak alkalmazást.

a. A vonatkozó törvényekkel és jogszabályokkal összhangban, a bizalmi munkakört betöltő személyzettel megfelelő módon közölni kell a munkakapcsolat befejeződése utáni időszakra is vonatkozó titoktartási kötelességeiket, valamint az ezen kötelességek be nem tartásának lehetséges következményeit.
b. A kilépő alkalmazottaknak vissza kell adniuk minden vállalati felszerelési tárgyat, és minden jogosultságukat vissza kell vonni,.
c. Az MSZ ISO/IEC 17799:2006 8.3-ben megadott intézkedéseket ajánlott alkalmazni.

5.6 Fizikai és környezeti biztonság

5.6.1 Biztonságos területek

Követelmény: Az ASZ-nek meg kell akadályoznia a jogosulatlan fizikai hozzáférést, a fizikai környezetben bekövetkezett károsodást, valamint a szervezet helyiségeit és információit meg kell védenie a nem megengedett külső hatásoktól..

a. Az ASZ rendszereit biztonságos körletekben kell elhelyezni, és az ilyen körletekbe való belépést a megfelelően feljogosított tisztviselőkre kell korlátozni.
b. A belépés időpontját, a tartózkodás célját, időtartamát, a kilépés időpontját naplózni kell.
c. Az MSZ ISO/IEC 17799:2006 9.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.6.2 Berendezések biztonsága

Követelmény: Az ASZ-nek meg kell akadályoznia a berendezések elveszését, károsodását, ellopását, a vagyontárgyak veszélyeztetését és a szervezet tevékenységének megszakítását.

a. Megfelelő intézkedéseknek kell létezniük az ASZ vagyontárgyainak védelmére a felszerelési tárgyakat és információt érintő véletlen és szándékos károk, pl. lopás és rongálás ellen, csakúgy, mint a szolgáltatás megfelelő folyamatosságának biztosítására.
b. Az MSZ ISO/IEC 17799:2006 9.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.7 Kommunikáció és üzemeltetés irányítása

5.7.1 Üzemeltetési eljárások és felelősségek

Követelmény: Az ASZ-nek biztosítania kell, hogy az információ-feldolgozó eszközök üzemeltetése helyes és biztonságos legyen.

a. Világos és részletes eljárásokat kell definiálni az ASZ bizalmi munkaköreire, amelyekben:
   - pontos felelősségek vannak megjelölve az üzemeltetést és az információ-feldolgozó berendezések menedzsmentjét illetően,
   - a feladatok megosztása részletezve van.
b. Megfelelő fegyelmi szankciókat kell alkalmazni azokkal a munkatársakkal szemben, akik megsértik az ASZ szabályzatait vagy eljárásait.

[Minősített]

a. Az ASZ-nek elegendő számú olyan munkatársat kell alkalmaznia, akik olyan szaktudás, tapasztalat és képzettség birtokában vannak, amelyek a felkínált szolgáltatásokhoz szükségesek, és a munkakörhöz megfelelnek

   A bizalmi munkakörök: csak olyan személyek tölthetik be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

   - Biztonsági tisztviselő: Az archiválási szolgáltatás biztonságáért általánosan felelős személy.
   - Rendszeradminisztrátor: Az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.
   - Rendszerüzemeltető: Az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.
   - Független rendszervizsgáló: Az archiválási szolgáltató naplózott, illetve archivált adatállományát (ide nem értve a szolgáltatás nyújtása keretében archiválásra átvett adatokat) vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

   Ajánlott bizalmi munkakör:

   - Archiválási tisztviselő: az archivált adatok kódolását és dekódolását, valamint az archivált elektronikus aláírások érvényességének folyamatos karbantartását és az archivált adatokkal kapcsolatos igazolások kiadását végző, illetve ezen tevékenységekért felelős személy,

[Nem minősített]

b. Az ASZ-nek elegendő számú olyan munkatársat kell alkalmaznia, akik olyan szaktudás, tapasztalat és képzettség birtokában vannak, amelyek a felkínált szolgáltatásokhoz szükségesek, és a munkakörhöz megfelelnek. Bizonyos, a rendszer megbízható üzemelése szempontjából kritikus feladatköröket (bizalmi munkaköröket) indokolt megfelelő megbízhatóságú személyekre (bizalmi tisztségviselőkre) bízni. A bizalmi munkakörök kialakításánál arra kell figyelemmel lenni, hogy egy szerepkör betöltőjének kezében ne egyesülhessenek a rendszer megbízható működése szempontjából összeférhetetlen funkciók:

   A bizalmi munkakörök: csak olyan személyek tölthetik be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja. A bizalmi munkakörök lehetséges kialakítására példaként szolgálhat az alábbi felosztás:

   biztonsági tisztviselő: az archiválási szolgáltatás biztonságáért általánosan felelős személy,

   rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy,

   rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy,

   archiválási tisztviselő: Archiválási tisztviselő: az archivált adatok kódolását és dekódolását, valamint az archivált elektronikus aláírások érvényességének folyamatos karbantartását és az archivált adatokkal kapcsolatos

igazolások kiadását végző, illetve ezen tevékenységekért felelős személy,

független rendszervizsgáló: az archiválási szolgáltató naplózott, illetve archivált adatállományait (ide nem értve a szolgáltatás nyújtása keretében archiválásra átvett adatokat) vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy,

c. Összeférhetetlenségek:
   - törekedni kell a bizalmi munkakörök teljes személyi elválasztására;
   - a biztonsági tisztviselő, vagy archiválási tisztviselő nem töltheti be a független rendszervizsgálói munkakört;
   - minősített szolgáltató esetén a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói munkakört.

d. A szolgáltatónak a szolgáltatások nyújtásához használt elektronikus aláírási termékeit elkülönítetten kell kezelnie és működtetnie az egyéb tevékenységeihez használt termékektől.
e. A biztonsági eseményekből és üzemzavarból származó kárt a legkisebbre kell csökkenteni az események jelentésével és válaszeljárások használatával.
f. Az MSZ ISO/IEC 17799:2006 10.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.7.2 Harmadik fél (alvállalkozók, közreműködők) szolgáltatásnyújtásának irányítása

Követelmény: Az ASZ-nek be kell vezetnie, és fenn kell tartania az információbiztonság és szolgáltatásnyújtás megfelelő szintjét, összhangban a harmadik fél szolgáltatásnyújtási megállapodásaival.

a. A harmadik felet igénybevevő szolgáltatónak ellenőriznie kell, hogy a harmadik fél, amely számára bizalmi szolgáltatásokat nyújt, eleget tesz-e minden szükséges kötelezettségének.
b. MSZ ISO/IEC 17799:2006 10.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.7.3 Rendszertervezés és elfogadása

Követelmény: Az ASZ minimalizálja a rendszerhibák kockázatát.

a. Az ASZ-nek előre meg kell terveznie a feldolgozó és tároló kapacitását abból a célból, hogy a tőle elvárható mértékben ki tudja elégíteni az előre tervezhető esetleges feldolgozási csúcsidőszakokat, és hogy betartsa kötelezettségvállalását a kezelendő dokumentumok mennyiségét illetően az elvárt tárolási időtartamban.
b. Az MSZ ISO/IEC 17799:2006 10.3-ban megadott intézkedéseket ajánlott alkalmazni.
c. A szóban forgó kapacitástervezést a rendszer beruházási költségek, a jogi büntető intézkedések, a biztosítási kötvény árak és a jó hírnév megrendülése mérlegelésével kell végrehajtani.

5.7.4 Védelem a rosszindulatú és mobil kódok ellen

Követelmény: Az ASZ-nek biztosítania kell a szoftverek és információk sértetlenségét.

a. Az MSZ ISO/IEC 17799:2006 10.4-ben megadott intézkedéseket ajánlott alkalmazni.

5.7.5 Mentés

Követelmény: Az ASZ-nek biztosítania kell az információk és az információ-feldolgozó berendezések sértetlenségét és rendelkezésre állását.

a. Az ASZ működésének újrakezdéséhez szükséges rendszeradatokat olyan biztonságos helyre kell elmenteni és helyen kell tárolni, amely alkalmas arra, hogy az ASZ rendkívüli események/katasztrófák esetén az üzemelést időben visszaállítsa.
b. A biztonsági mentési és helyreállítási funkciókat az 5.7.1 szakaszban előírt megfelelő bizalmi szerepkörök által kell megvalósítani.
c. Megfelelően kiépített és felszerelt háttér-tároló helyekről ajánlott gondoskodni, illetőleg szükség esetén a visszaállítási terv lépéseit kell alkalmazni.
d. A szóban forgó mentési rendszer méretezésénél mérlegre kerülhet a beruházási költség, a kapcsolódó biztosítás költsége, azok a bírságok és kötbérek, amelyek a kívánt dokumentumok bemutathatatlansága esetén lépnek életbe, és az a költség is, amely meg nem fogható értékekben testesül meg, mint például a szervezet hírneve.
e. Az MSZ ISO/IEC 17799:2006 10.5-ben megadott intézkedéseket ajánlott alkalmazni.

5.7.6 Hálózatbiztonság kezelése

Követelmény: Az ASZ-nek biztosítania kell a hálózati információbiztonságot és a támogató infrastruktúra védelmét.

a. A hálózatokat védeni kell a dokumentumok kiadása és tárolása tekintetében annak biztosítására, hogy illetéktelen adat ne kerülhessen be a dokumentum kiadási vagy tárolási folyamatba, és ne kerülhessen törlésre onnan, illetve semmilyen bizalmas információ ne kerüljön felfedésre.
b. Az MSZ ISO/IEC 17799:2006 10.6-ban megadott intézkedéseket ajánlott alkalmazni.

5.7.7 Adathordozók kezelése

Követelmény: Az ASZ-nek meg kell gátolnia az adathordozók és a hordozott információk jogosulatlan módosítását, eltávolítását, hozzáférhetetlenné tételét vagy tönkretételét, illetve az információk jogosulatlan felfedését, így az üzleti tevékenység félbeszakadását.

a. Az adathordozók védelmét érvényre kell juttatni azok teljes kezelési folyamata során, hogy biztosítva legyen a tartalmuk sértetlensége és bizalmassága a beszerzésüktől/átadásuktól kezdődően a tárolásukon és telepítésükön (ha van ilyen) keresztül egészen a leselejtezésükig.
b. Az adathordozó-kezelési eljárásoknak védeniük kell a hordozók elavulása és elhasználódása ellen, a feljegyzések köteles megőrzési időszakán belül.
c. Az MSZ ISO/IEC 17799:2006 10.7-ben megadott intézkedéseket ajánlott alkalmazni.

5.7.8 Információcsere

Követelmény: Az ASZ-nek biztosítania kell a szervezeten belüli és bármely külső entitással történő információ- és szoftvercsere biztonságát.

a. Az MSZ ISO/IEC 17799:2006 10.8-ban megadott intézkedéseket ajánlott alkalmazni.

5.7.9 Elektronikus kereskedelmi szolgáltatások

Követelmény: Az ASZ-nek gondoskodnia kell az elektronikus kereskedelmi szolgáltatás biztonságáról és biztonságos használatáról.

a. MSZ ISO/IEC 17799:2006 10.9-ben megadott intézkedéseket ajánlott alkalmazni.

5.7.10 Figyelemmel kísérés (Monitoring)

Követelmény: Az ASZ-nek képesnek kell lennie a jogosulatlan információ-feldolgozó tevékenység felfedésére.

a. A naplózott adatállomány bejegyzéseit védeni kell a módosítástól.
b. Az átvilágítási naplókat figyelni kell, vagy rendszeresen át kell vizsgálni, hogy azonosítsák a rosszindulatú tevékenység bizonyítékait.
c. Az ASZ-nek olyan átvilágítási eljárásokat kell alkalmaznia a rendszer üzemeltetése alatt, amelyek biztosítják, hogy az archiválási szolgáltatásra vonatkozó minden lényeges információt megfelelő hosszúságú ideig feljegyeznek, elsősorban azért, hogy jogi eljárásokhoz az archivált dokumentum bizonyítékul szolgálhasson.
d. Folyamatos figyelő és riasztó segédeszközöket kell biztosítani, amelyek lehetővé teszik az ASZ számára, hogy az erőforrásaihoz való hozzáférésre irányuló mindenfajta jogosulatlan és/vagy szabálytalan kísérletet időben érzékeljen, feljegyezzen, és arra reagáljon.
e. Az MSZ ISO/IEC 17799:2006 10.10-ben megadott intézkedéseket ajánlott alkalmazni.

5.8 Hozzáférés-ellenőrzés

5.8.1 Működési követelmények a hozzáférés-ellenőrzéshez

Követelmény: Az ASZ-nek szabályoznia kell az információhoz való hozzáférést.

a. Az MSZ ISO/IEC 17799:2006 11.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.8.2 A felhasználó hozzáférésének kezelése

Követelmény: Az ASZ-nek biztosítania kell az információs rendszerhez való jogosult felhasználói hozzáférést, illetve meg kell gátolnia a jogosulatlan hozzáférést.

a. Az informatikai rendszer minden felhasználójának és az adminisztratív folyamatok minden szereplőjének személy szerint azonosítottnak kell lennie.
b. Az archiválási szolgáltatás a felek megállapodása alapján oly módon is nyújtható, hogy az adatgazda nem bocsátja a szolgáltató rendelkezésére személyazonosító adatait.
c. Az MSZ ISO/IEC 17799:2006 11.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.8.3 Jogosulatlan hozzáférés megakadályozása

Követelmény: Az ASZ-nek meg kell akadályoznia a jogosulatlan felhasználói hozzáférést, az információ és információ-feldolgozó eszközök veszélyeztetését vagy lopását.

a. A külső és belső jogosult felhasználókkal írásban közölni kell a felelősségüket és az együttműködésük szükségességét a jogosulatlan hozzáférések meggátolásának céljából. Ahol ez alkalmazható, érvényre kell juttatni az „Üres asztal, üres képernyő” szabályt.
b. Az MSZ ISO/IEC 17799:2006 11.3-ban megadott intézkedéseket ajánlott alkalmazni.

5.8.4 Hálózati hozzáférés ellenőrzése

Követelmény: Az ASZ-nek meg kell akadályoznia a hálózati szolgáltatásokhoz való jogosulatlan hozzáférést.

a. Az MSZ ISO/IEC 17799:2006 11.4-ben megadott intézkedéseket ajánlott alkalmazni.

5.8.5 Az operációs rendszerhez való hozzáférés ellenőrzése

Követelmény: Az ASZ-nek meg kell akadályoznia az operációs rendszerekhez való jogosulatlan hozzáférést.

a. A naplókat megfelelően kell védeni és átvizsgálni.
b. Az MSZ ISO/IEC 17799:2006 11.5-ben megadott intézkedéseket ajánlott alkalmazni.

5.8.6 Az alkalmazás- és információ-hozzáférés ellenőrzése

Követelmény: Az ASZ-nek meg kell akadályoznia az alkalmazási rendszerekben őrzött információhoz való jogosulatlan hozzáférést

a. Az ASZ-nek biztosítania kell, hogy a hozzáférés-ellenőrzési szabályzattal összhangban korlátozza az információkhoz és alkalmazási rendszer funkcióihoz való hozzáférést, és hogy az ASZ rendszere elegendő számítógépes biztonsági ellenőrzést nyújt a szabályzatában azonosított bizalmi szerepkörök szétválasztásához. Különösen a rendszer segédprogramjainak használatát kell korlátozni és ellenőrizni. A hozzáférést korlátozni kell, csak annyi hozzáférést engedve az erőforrásokhoz, amennyi az adott felhasználónak kijelölt szerepkör(ök) betöltéséhez szükséges.
b. Az MSZ ISO/IEC 17799:2006 11.6.1-ben megadott intézkedéseket ajánlott megvalósítani a tárolást illetően.
c. Az MSZ ISO/IEC 17799:2006 11.6.2-ben megadott intézkedéseket ajánlott megvalósítani az aláírási kulcsokkal kapcsolatban.

5.8.7 Mobil számítógép használata és távmunka

Követelmény: Az ASZ-nek gondoskodnia kell az információbiztonságról mobil számítástechnikai és távmunka végzéséhez használt berendezések esetén.

a. Az MSZ ISO/IEC 17799:2006 11.7-ben megadott intézkedéseket ajánlott alkalmazni.

5.9 Információs rendszerek beszerzése, fejlesztése és karbantartása

5.9.1 Információs rendszerek biztonsági követelményei

Követelmény: Az ASZ-nek biztosítania kell, hogy az információs rendszerek szerves része legyen a biztonság.

a. Az implementációs hibákat ajánlott olyan szoftverek és hardverek használatával csökkenteni, amelyeket egy nemzetközileg elfogadott biztonsági követelmény-rendszer szerint értékeltek és minősítettek (CC, ITSEC, FIPS).
b. Az ASZ-nek olyan megbízható rendszereket és termékeket kell használnia, amelyek módosítás ellen védettek.
c. A biztonsági követelményeket elemezni kell mindenfajta, az ASZ által vagy az ASZ nevében vállalt rendszerfejlesztési projekt tervezési és követelmény-előírási szakaszában, biztosítva, hogy a biztonság beépüljön az informatikai rendszerekbe.
d. Az MSZ ISO/IEC 17799:2006 12.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.9.2 Helyes információfeldolgozás az alkalmazásokban

Követelmény: Az ASZ-nek intézkedéseket kell tennie az alkalmazásokban lévő információ sérülésének, elvesztésének, jogosulatlan módosításainak vagy az ezekkel való visszaélések meggátolása érdekében.

a. Az MSZ ISO/IEC 17799:2006 12.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.9.3 Kriptográfiai intézkedések

Követelmény: Az ASZ-nek az információ bizalmasságát, hitelességét és sértetlenségét védenie kell kriptográfiai eszközökkel.

a. Az ASZ köteles rendszeresen felülvizsgálni a biztonságosnak elfogadott, elektronikus aláírással kapcsolatos kriptográfiai algoritmusok és paraméterek listáját, ehhez figyelembe kell vegye a Hatóság határozatait, illetve más mértékadó testületek állásfoglalásait.
b. Amennyiben az ASZ az „archivált adat titkosított formában való tárolásának biztosítása” kiegészítő szolgáltatást is nyújta, az alkalmazott titkosító algoritmusok, kulcsméretek, kulcselőállítási módszerek, kulcskezelési eljárások megfelelőségéről (megbízhatóságáról, s ezek megvalósításának helyességéről) a nemzetközi kriptográfiai szakmai elvárásokon alapuló szakértői véleményt vagy tanúsító szervezet által kiadott igazolást kell beszereznie.
c. Az MSZ ISO/IEC 17799:2006 12.3-ban megadott intézkedéseket ajánlott alkalmazni.

5.9.4 A rendszerállományok biztonsága

Követelmény: Az ASZ-nek biztosítania kell a rendszerállományok biztonságát.

a. Az MSZ ISO/IEC 17799:2006 12.4-ben megadott intézkedéseket ajánlott alkalmazni.

5.9.5 Biztonság a fejlesztés és támogató folyamatokban

Követelmény: Az ASZ-nek fenn kell tartania az alkalmazási rendszer szoftverének és információinak biztonságát.

a. Az alkalmazásokat jól definiált biztonsági eljárásoknak megfelelően kell kifejleszteni, tesztelni és üzembe helyezni.
b. Létezzenek változtatás-ellenőrzési eljárások mindenfajta, működéshez szükséges rendszer komponens új kiadásaira, módosításaira és gyors javításaira.
c. Az MSZ ISO/IEC 17799:2006 12.5-ben megadott intézkedéseket ajánlott alkalmazni.

5.9.6 Műszaki sebezhetőség kezelése

Követelmény: Az ASZ-nek intézkedéseket kell tennie a nyilvánosságra hozott műszaki sebezhetőségek kiaknázásából származó kockázatok csökkentése érdekében.

a. Az MSZ ISO/IEC 17799:2006 12.6-ban megadott intézkedéseket ajánlott alkalmazni.

5.10 Az információbiztonsági incidensek kezelése

5.10.1 Az információbiztonsági események és gyenge pontok jelentése

Követelmény: Az ASZ-nek biztosítania kell az információs rendszerekhez kapcsolódó információbiztonsági események és gyenge pontok felismerésének olyan módját, ami lehetővé teszi a helyesbítő tevékenységek időben való megtételét.

a. Az ASZ-nek időben és egyeztetett módon kell cselekednie, hogy gyorsan válaszoljon az eseményekre, és korlátozza a biztonság megsértésének hatását. Minden eseményt jelenteni kell a biztonsági tisztviselőnek az előfordulást követő legrövidebb időn belül.
b. Az MSZ ISO/IEC 17799:2006 13.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.10.2 Az információbiztonsági incidensek és fejlesztések kezelése

Követelmény: Az ASZ-nek biztosítania kell, hogy konzisztens és hatékony megoldásokat alkalmaz az információbiztonsági incidensek kezelésére.

a. Az MSZ ISO/IEC 17799:2006 13.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.11 Működés folytonosság irányítása

5.11.1 A működés folytonosság irányításának információbiztonsági szempontjai

Követelmény: Az ASZ-nek intézkedéseket kell tennie az információs rendszerek jelentős hibáiból vagy összeomlásából származó, üzleti tevékenységek félbeszakadását eredményező rendkívüli események elhárítása és a kritikus fontosságú üzleti folyamatok megvédése érdekében, valamint biztosítania kell az időben történő visszaállítást.

a. Az ASZ-nek olyan folytonossági tervet kell meghatároznia és fenntartania, amelynek végrehajtását katasztrófa esetén rendelik el.
b. **[Minősített]** Biztosítani kell, hogy az őrzésében lévő érvényességi lánc, illetve az igazolások jogosultak kérésére történő kiadása szolgáltatás eseti kiesésének időtartama nem haladhatja meg a három napot.
b. **[Nem minősített]** Az ASZ a szolgáltatásra irányadó szabályzataiban határozza meg, hogy az őrzésében lévő érvényességi lánc, illetve az igazolások jogosultak kérésére történő kiadása szolgáltatás eseti kiesésének időtartama legfeljebb mennyi lehet.
c. Az archiválási szolgáltató tevékenységéből csak az adatok megőrzésre átvételét szüneteltetheti.
d. Az MSZ ISO/IEC 17799:2006 14.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.12 Megfelelőség

5.12.1 Megfelelések a jogi követelményeknek

Követelmény: Az ASZ-nek intézkedéseket kell tennie bármely jogszabály, szabályozó, vagy szerződésben meghatározott kötelezettség és bármely biztonsági követelmény megszegésének elkerülése érdekében.

a. A szolgáltatási szerződést oly módon kell megkötni, hogy a szerződés tartalma az elektronikus dokumentumokban szereplő személyes adatok vonatkozásában kielégítse a személyes adatok védelméről szóló törvény által az adatfeldolgozás vonatkozásában meghatározott feltételeket.
b. Az MSZ ISO/IEC 17799:2006 15.1-ben megadott intézkedéseket ajánlott alkalmazni.

5.12.2 A biztonsági szabályzatoknak és szabványoknak való megfelelés és műszaki megfelelés

Követelmény: Az ASZ-nek biztosítania kell a rendszerek megfelelését a szervezeti biztonsági szabályzatoknak és szabványoknak.

a. A biztonsági szabályzatoknak való megfelelésnek teljesülnie kell.
b. Az MSZ ISO/IEC 17799:2006 15.2-ben megadott intézkedéseket ajánlott alkalmazni.

5.12.3 Az információs rendszerek auditálási szempontjai

Követelmény: Az ASZ-nek intézkedéseket kell tennie a rendszeraudit folyamat hatékonyságának maximalizálása és a belőle származó, illetve a rendszeraudit folyamatot hátrányosan befolyásoló zavarás legkisebb mértékűre szorítása érdekében.

a. Léteznie kell egy megfelelő audit eljárásnak még akkor is, ha erre vonatkozóan nincsen speciális jogi követelmény.
b. Az MSZ ISO/IEC 17799:2006 15.3-ban megadott intézkedéseket ajánlott alkalmazni.

6 Megfelelőségi követelmények

Az ASZ-nek be kell mutatnia, hogy:

a. eleget tesz a 3.1 fejezetben definiált kötelezettségeinek;
b. megvalósított olyan óvintézkedéseket, amelyek megfelelnek a követelményeknek, beleértve azokat, amelyek a jelen dokumentumnak megfelelően az ASZ által nyújtott szolgáltatásokra vonatkoznak.

Megjegyzés: Ez megvalósítható például egy elektronikus aláírás szolgáltatási szakértő olyan szakértői véleményével, melyet alátámasztanak tanúsító szervezetek által kiadott igazolások, részben az MSZ ISO/IEC 27001:2006-tal való összhangról, részben a műszaki biztonsági követelményeknek való megfelelésről..

7 Hivatkozások

- 2001. évi XXXV. törvény az elektronikus aláírásról
- 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
- 3/2005. (III. 18.) IHM rendelet - az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 114/2007. (XII. 29.) GKM rendelet – a digitális archiválás szabályairól
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára
- CWA 15579 E-invoices and digital signatures
- CWA 15580 Storage of Electronic Invoices
- CWA 14171:2004 General guidelines for electronic signature verification
- ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates
- ETSI TS 102 573 (V0.0.5, 2007-05) Policy requirements for trust service providers signing and/or storing data relevant for accounting
- RFC draft: Long-Term Archive Service Requirements
- MSZ ISO/IEC 17799:2006 Az információbiztonság irányítási gyakorlatának kézikönyve
- MSZ ISO/IEC 27001:2006 Az információbiztonság irányítási rendszerei.
- Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre (NHH)

8 Rövidítések

CEN	Comité Européen de Normalisation	Európai Szabványügyi Bizottság
CWA	CEN Workshop Agreement	CEN munkacsoport megállapodás
ETSI	European Telecommunication Standards Institute	Telekommunikációs Szabványok Európai Intézete
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
RFC	Request for Comment	felhívás véleményezésre
ASZ		archiválási szolgáltató