A kormányzati kommunikációs beszerzések
során alkalmazandó akkreditált informatikai rendszerrel
kapcsolatos
Követelmények

I. Az informatikai rendszerrel szembeni műszaki követelmények

Az informatikai rendszerrel kapcsolatos általános követelményeket találhatjuk ebben a fejezetben. Az első alfejezet a kormányzati kommunikációs beszerzések során alkalmazható informatikai rendszerrel szemben támasztott követelményekről szóló 1/2016. (II. 1.) MK rendeletben (a továbbiakban: MK rendelet) tételesen meghatározott műszaki követelmények részletezését tartalmazza. A további alfejezetek a követelményekhez kapcsolódó részletesebb biztonsági és funkcionális elvárásokat írják le.

I.1. A jogszabályi elvárásokkal kapcsolatos követelmények

Az alábbiakban az MK rendeletben tételesen megfogalmazott elvárások és követelmények pontosítását adjuk meg a rendeletben szereplő szerkezetnek megfelelően. Az egyes későbbi fejezetek az alábbi elvárásokat tovább részletezhetik még.

I.1.1. Az informatikai rendszerrel szemben támasztott részletes műszaki paraméterek

Az MK rendelet 3. § értelmében az informatikai rendszernek műszakilag a következő követelményeknek és részletes műszaki paramétereknek kell megfelelnie:

a) az informatikai rendszer vékony klienses reszponzív - azaz hordozható és asztali eszközökön is használható - webes felületet biztosít a felhasználók számára:

Az informatikai rendszernek olyan vékony kliens megoldást kell alkalmaznia, amelynek használatához a felhasználóknak semmilyen speciális alkalmazást nem kell telepíteni. Az informatikai rendszernek használhatónak kell lennie minden elterjedt böngésző alkalmazással.

A vékony kliens megoldásnak reszponzívnak kell lennie, azaz minden elterjedt asztali képernyő felbontáson, tablet eszköz és mobil készülék képernyő felbontáson azonos és teljes funkcionalitással kell működnie. Ipari sztenderd technológiák felhasználásán keresztül (mint pl. HTML5, JavaScript, jQuery, AJAX), a felhasználói felület lehető legszélesebb körű támogatása szükséges.

b) az informatikai rendszer biztonságos kapcsolaton keresztül kommunikál:

Az informatikai rendszernek biztonságos, HTTPS csatornán keresztül elérhetőnek kell lennie a felhasználók számára. A HTTPS tanúsítványnak hivatalos, nyilvántartásba vett hitelesítési szolgáltatótól kell származnia. A HTTP kommunikáció védelmére SSL vagy TLS réteg beiktatása szükséges, amely szavatolja, hogy a felhasználó adatforgalmát harmadik fél nem láthatja, illetve garantálja, hogy az adatforgalmazás valóban az informatikai rendszer által biztosított szolgáltatási felületeken keresztül történik. A biztonságos kommunikáció védelmet nyújt az adathalászat és a közbeékelődéses támadások ellen. Az informatikai rendszer által alkalmazott SSL tanúsítványnak meg kell felelnie az SSL szabvány hitelesítési eljárásának. A rendszer minden gépi interfészét úgy kell kialakítani, hogy az biztonságos csatornán keresztüli adatkommunikációra legyen képes. A kommunikációs csatornának biztosítania kell az adatok hitelességét, sértetlenségét és bizalmasságát is.

c) az informatikai rendszer jogosultságkezeléssel rendelkezik, amely biztosítja, hogy csak az illetékes felhasználók férhessenek hozzá az adatokhoz:

Az informatikai rendszer jogosultság kezelésének garantálnia kell, hogy az egyes felhasználók csak a saját szerepkörüknek megfelelő adatokhoz férhessenek hozzá (olvasási, írási, törlési műveletekre egyaránt). A rendszernek továbbá biztosítania kell azt is, hogy az egyes felhasználók csak a saját szervezetükhöz kapcsolódó adatokhoz férhessenek hozzá (olvasási, írási, törlési műveletekre egyaránt).

Az informatikai rendszernek biztosítania kell a végfelhasználók rögzítését, amely során a végfelhasználói fiók és annak jogosultsági szintje kerül rögzítésre. A végfelhasználók az informatikai rendszert a felhasználónevük és a jelszavuk megadásával érhetik el. Az informatikai rendszernek biztosítania kell, hogy paraméterezhető inaktivitási idő után a bejelentkezést ismételten el kelljen végezni, továbbá garantálnia kell a felhasználói fiókok bejelentkezési adatai (kiemelten jelszavak) paraméterezhető időközönkénti megváltoztatását. Az informatikai rendszer biztosítja, hogy a bejelentkezett felhasználó kizárólag a szerepköréhez és jogosultsági szintjéhez megfeleltethető funkciókat érhessen el.

d) az informatikai rendszer lehetőséget biztosít a meglévő informatikai rendszerekkel való szabványos interfészen keresztül megvalósított interoperabilitásra:
Az informatikai rendszernek szabványos interfészeket kell biztosítani a külső kapcsolódó rendszerekkel való együttműködéshez. Ennek megvalósításához az informatikai rendszernek képesnek kell arra lennie, hogy SOAP és HTTP REST hívásokon küldjön vagy fogadjon adatokat a kapcsolódó rendszerekből. A kommunikáció csatornája webes felületen megvalósított szolgáltatás, amelynek biztonságáról a HTTPS és a felhasználói azonosítás segítségével kell gondoskodni.
Az adatok átadása során egyedi adatformátum nem használható. Az adatokat XML és JSON formátumban kell tudni az interfészeken átadni és fogadni.

e) az informatikai rendszerre vonatkozóan felhasználói, fejlesztői és üzemeltetési dokumentáció áll rendelkezésre:
Az informatikai rendszernek teljes körű felhasználói, fejlesztői és üzemeltetési dokumentációval kell rendelkeznie.
Felhasználói kézikönyv: a rendszernek minden egyes szerepkörhöz önálló felhasználói kézikönyvet kell nyújtania. A felhasználói kézikönyv a végfelhasználó által elvégezhető feladatokat mutatja be részletesen. A kézikönyvnek minden olyan információt tartalmaznia kell, amely ahhoz szükséges, hogy egy informatikában hétköznapi, alapszinten járatos felhasználó egyedül is, külső segítség nélkül elboldoguljon. A kézikönyv letölthető formában is rendelkezésre kell álljon, de emellett az informatikai rendszer ezt súgóként is nyújthatja.
Fejlesztői kézikönyv: A fejlesztői kézikönyv tartalmaznia kell a rendszer architekturális és interfész leírásait, terv dokumentumait és tesztelési dokumentumait. A fejlesztői dokumentáció a rendszer belső összefüggéseit, illetve implementációját írja le. A kézikönyv célja, hogy biztosítsa az informatikai rendszer átgondolt, tervezett, pontosan implementált és tesztelt módon történő elkészítését, így csökkentve az esetleges fejlesztési hibákból eredő problémák kockázatát.
Üzemeltetési kézikönyv: A kézikönyvnek minden olyan üzemeltetési eljárást, információt és megoldást tartalmaznia kell, ami alapján egy informatikai üzemeltetésben járatos – de a fejlesztésben szerepet nem vállaló – szakember (szakember csapat) képes önállóan, fejlesztői segítség nélkül működtetni a rendszert. Az üzemeltetési dokumentáció a rendszeradminisztrátor és az alkalmazásadminisztrátor feladatait és azok ajánlott megoldását fejti ki. A kézikönyv célja, hogy biztosítsa az informatikai rendszer átgondolt és tervezett üzemeltetését, így csökkentve az esetleges üzemeltetési hibákból eredő problémák kockázatát.

Az *MK rendelet 4. § értelmében az informatikai rendszert támogató informatikai infrastruktúrát a következő követelményeknek és részletes műszaki paramétereknek megfelelően kell kialakítani:*

a) naptári évenként legalább tízezer beszerzési eljárás adatainak tárolására és folyamatainak kezelésére alkalmas:
Az informatikai rendszert úgy kell méretezni, hogy az képes legyen naptári évenként legalább tízezer beszerzési eljárás adatainak tárolására és kezelésére. Évi tízezer beszerzési eljárás esetén az informatikai rendszer által nyújtott felhasználói és szolgáltatási felületeken keresztül, azok adatainak elérését elfogadható időn belül kell biztosítani. A rendszerek nemcsak a 10.000/365 db napi egyenletesen bekerülő adatmennyiséget kell tudnia kezelni, hanem csúcsidőkben napi 500 beszerzési eljárás adatának fogadását és kezelését is.

b) az informatikai rendszeren keresztül továbbított (küldött és fogadott) adatok archiválására és tárolására a 2. §-ban meghatározott paraméterek szerint alkalmas:
Az informatikai rendszer által kezelt adatok fizikai törlése nem megengedett, helyette az adatok archiválása szükséges. Az archív adatok hozzáférését minimálisan az adott pénzügyi év lezárásáig teljes körűen kell biztosítani. Az archivált Beszerzések teljes életciklusa alatt keletkezett adatokhoz való hozzáférés biztosítandó.
A már nem élő, de még megőrzött beszerzések adataira olyan visszaállítási eljárásokat kell alkalmazni, amelyek garantálják, hogy minden adat 1 napon belül újra elérhető legyen.

c) az informatikai rendszerhez való hozzáférés teljes körű naplózása biztosított:
Az informatikai rendszernek naplóinak tartalmazniuk kell az alábbi információkat:

- melyik felhasználó
- mikor
- milyen adaton
- milyen műveletet hajtott végre

Az informatikai rendszernek minimálisan az alábbi eseményeket kell naplóznia:

- rendszer indulása és leállása
- felhasználói belépések és kilépések (sikeres és sikertelen egyaránt)
- összes beszerzéshez kapcsolódó adaton végzett felhasználó művelet (megtekintés, létrehozás, módosítás, törlés)
- jogosultságokon és felhasználói adatokon végzett összes művelet (megtekintés, létrehozás, módosítás, törlés)
- hiba események

A naplóbejegyzéseket az archiválási idővel megegyező ideig és módon kell tárolni.

d) az informatikai rendszerről rendszeres biztonsági mentés készül, amely alapján visszaállítható egy korábbi állapot:
Az informatikai rendszer adatmentéseinek biztosítaniuk kell, hogy a tárolási idő végezetéig minden kezelt adat konzisztens állapota visszaállítható legyen hiba esetén. A mentéseknek a beszerzések adatai mellett ki kell terjedniük a rendszer naplóira is. Az adatok biztonsági mentése legalább hetente szükséges.

e) az informatikai rendszer 99,9%-os rendelkezésre állást nyújt munkanapokon a 6 és 20 óra közötti időszakban:
Az informatikai rendszernek 99,9%-os rendelkezésre állást kell biztosítania havi szinten (azaz minden naptári hónapban a munkanapokra vonatkoztatott 6-20 óra idősávban a rendszer maximum 0,1% időtartamra lehet fizikailag vagy funkcionálisan elérhetetlen). A rendelkezésre állásba az ütemezett és a nem ütemezett (hibákból eredő) leállást is bele kell érteni. A rendelkezésre állási követelmények csak akkor tekinthetők teljesültnek, ha a rendszer teljes funkcionalitása elérhető és működőképes.

I.2. Dokumentálással kapcsolatos követelmények

Az MK rendelet 3. § e) pontja értelmében az informatikai rendszernek többek között 1) felhasználói, 2) fejlesztői és 3) üzemeltetői dokumentációval kell rendelkeznie. A dokumentációval kapcsolatos általános formai követelmények az első alfejezetben kerülnek rögzítésre. Az 0. és további alfejezetek a konkrét tartalmi követelményeket tartalmazzák. A dokumentumok számát és struktúráját szabadon megválaszthatja az üzemeltető, de tartalmilag minden elemet tartalmaznia kell a teljes dokumentációhalmaznak.

I.2.1. Formai követelmények

Az infokommunikációs rendszer dokumentálása során az alábbi pontokban részletezett formai elemeket minden dokumentumban értelemszerűen kell szerepeltetni.

- Dokumentum adatlap:
    - Dokumentum címe
    - Dokumentum tárgya
    - Fájl neve és verziója
    - Dokumentum típusa
    - Dokumentum verziószáma
    - Dokumentum státusza
    - Dátum
    - Készítő

    - Ellenőr
- Minősítés
- Lapszámozás
- Tartalomjegyzék
- Tárgymutató

I.2.2. Dokumentumok rendelkezésre állása

Az infokommunikációs rendszer dokumentációinak

- egy eredeti nyomtatott példányban papír alapon,
- egy szerkeszthető Microsoft Word formátumban elektronikus formában,
- egy nyomtatható PDF formátumban elektronikus formában

kell rendelkezésre állnia a rendszer üzemeltetőjénél.

I.2.3. Követelményspecifikáció

A követelményspecifikációnak tartalmaznia kell mindazokat az elvárásokat, amelyeket jelen dokumentum megfogalmaz a bevezetendő informatikai alkalmazással/rendszerrel szemben.
A követelményspecifikációnak a következőket kell tartalmaznia:

- Feladat meghatározás;
- A funkcionális megoldás összefoglalása;
- Technológiai követelmények;
- Oktatási követelmények.

A követelményspecifikációval szemben támasztott követelmények a következők:

- A követelményspecifikációnak teljesnek kell lennie, azaz tartalmaznia kell a jelen dokumentumban megfogalmazott valamennyi elvárást.
- Ne tartalmazzon a megoldás módjára vonatkozó szükségtelen megszorítást.
- Következetes kifejezésekkel, szóhasználattal, világos ábrákkal szemléltesse a folyamatokat.
- Ki kell terjednie minden támogatni kívánt folyamatra.
- Nem szabad egymásnak ellentmondó követelményeket megfogalmazni.

A követelményspecifikáció lehet jelen dokumentum másolata, kivonata, vagy tetszőleges más, a jelenlegitől független dokumentum.
Felhasználói dokumentáció – Felhasználói kézikönyv
A felhasználói dokumentáció egy adott rendszerelem szakszerű és üzembiztos használatának módját írja le a végfelhasználók által érthető módon. Az akkreditált informatikai rendszerre, rendszerelemre vagy szolgáltatásra vonatkozó felhasználói dokumentáció minden esetben követelmény. A felhasználói dokumentáció tartalmazza:

- a funkciók felhasználói leírása képekkel illusztrálva,
- a kezelési felületek, menürendszer ismertetését,
- az interfész leírásokat,
- a funkcióleírásokat, a funkciójegyzéket,
- a kapcsolódó rendszerelemek pontos hivatkozását,
- az ellenőrzési és hibakezelési eljárásokat / hibajegyzéket,
- logikai védelmi megoldások ismertetését.
- a rendszer felhasználói által is elérhető biztonsági funkciók leírását, a használat módját, esetleges beállításokat, azok megengedett módosításait;
- a rendszer biztonságos használatának szabályait és módszereit,
- a felhasználó felelősségét és kötelességeit a rendszer vagy rendszerelem biztonságának fenntartásához.

Az üzemeltető kötelessége a felhasználói dokumentációt a Nemzeti Kommunikációs Hivatal, az érintett szervezetek, a szállítók és más felhasználók rendelkezésére bocsátani, illetve a szükséges oktatásokat biztosítani az érintett kollégák számára.
Az akkreditált informatikai rendszer kapcsolódó dokumentációját a felhasználók az akkreditált informatikai rendszerben az érintett rendszerelem használatba vétele előtt megismerik. A megismerést az érintettek aláírásukkal igazolják.

I.2.4. Üzemeltetői dokumentáció – Üzemeltetési kézikönyv

Az üzemeltetési dokumentáció egy adott rendszerelem működtetésére, karbantartására és felügyeletére vonatkozó utasításokat tartalmazza az üzemeltetési feladatokat végző munkatársak által érthető módon. A Nemzeti Kommunikációs Hivatal minden esetben megköveteli az akkreditált informatikai rendszerre, rendszerelemre, vagy szolgáltatásra vonatkozó üzemeltetői dokumentációt. Az üzemeltetési dokumentáció tartalmazza:

- a technikai környezet ismertetését,
- a kapacitástervezési leírást,
- az alkalmazott portok, szolgáltatások, és protokollok részletes ismertetése,
- a kommunikációs környezet ismertetését,
- a szerepköröket és hozzájuk tartozó feladatok ismertetését,
- a jogosultsági rendszer részletes ismertetését,
- a feldolgozások részletes ismertetését üzemeltetési szempontból,
- a mentés, archiválás, monitorozás ismertetését,
- az időszaki teendők ismertetését,
- a hibaüzenetek, hibaelhárítással kapcsolatos feladatok ismertetését.
- biztonsági funkciók leírását megfelelő beállítását, alkalmazását, hibakezelést,
- a dokumentáció elkészültekor a beszerzett akkreditált informatikai rendszerben megtalálható ismert sérülékenységeket, azok pontos leírását, ez esetlegesen alkalmazható védelmi intézkedéseket.

Az üzemeltető kötelessége az üzemeltetői dokumentációt az érintettek rendelkezésére bocsátani, illetve a szükséges oktatásokat biztosítani.
Az akkreditált informatikai rendszer üzemeltetési dokumentációját az üzemeltetők az akkreditált informatikai rendszerben az érintett rendszerelem használatba vétele előtt megismerik. A megismerést az érintettek aláírásukkal igazolják.

I.2.5. Fejlesztői (Rendszer-) dokumentáció

A rendszerdokumentáció egy adott rendszerelem ismertetését tartalmazza az alkalmazásfejlesztők által érthető módon. A rendszerdokumentáció tartalmazza:

- a logikai adatmodellt, az egyedleírásokat, a struktúra ábrákat,
- a fizikai adatmodellt, az adatleírásokat, az adatjegyzéket,
- a feldolgozási folyamatok részletes ismertetését,
- a külső / belső rendszerkapcsolatok részletes ismertetését,
- az I/O adatszerkezetek ismertetését,
- az egyéb környezeti / kapcsolati feltételek ismertetését,
- a hibaelhárítással kapcsolatos feladatok ismertetését,
- az alkalmazott preventív, detektáló és javító védelmi eljárások ismertetését,
- az audit üzenetek / naplózás ismertetését.

Az üzemeltető kötelessége az fejlesztői dokumentációt az érintettek rendelkezésére bocsátani, illetve a szükséges oktatásokat biztosítani.
Az akkreditált informatikai rendszer fejlesztői dokumentációját a fejlesztők az akkreditált informatikai rendszerben az érintett rendszerelem módosítása/kifejlesztése előtt megismerik. A megismerést az érintettek aláírásukkal igazolják.

I.2.6. Megfelelőségi nyilatkozat

A fejlesztő/szállító ebben a dokumentumban nyilatkozik arról, hogy az általa biztosított szolgáltatás (az akkreditált informatikai rendszer):

- mindenben megfelel a vonatkozó előírásokban foglaltaknak, az előírások megsértése esetére akár anyagi kártérítési felelősséget is vállal
- a termék jogszabálykövetésére annak működési ideje alatt garanciát vállal,
- az esetlegesen felmerülő kiegészítő fejlesztéseket az adott rendszer keretein belül el tudja végezni.

A megfelelőségi nyilatkozatot a szolgáltatás üzemszerű használata előtt a Nemzeti Kommunikációs Hivatal részére rendelkezésre kell bocsátania az üzemeltetőnek.

I.3. Tervezés

Az üzemeltető köteles átadni a Nemzeti Kommunikációs Hivatal részére az akkreditált informatikai rendszer kapcsolódásait és kapcsolatait ábrázoló műszaki dokumentációt. Az egyes kapcsolatok vonatkozásában dokumentálni kell (írásban rögzíteni kell), hogy milyen biztonsági funkciók kerültek beépítésre, így például:

- Integritás biztosítása (például az integritást hardveres (RAID) és szoftveres (xy adatbázis-kezelő integritásvédelme, valamint jogosultságkezelés)
- Azonosítás, hitelesítés (a kapcsolódó követelményeket az azonosítás és hitelesítésre vonatkozó pontban definiáljuk), annak konfigurációs megvalósítása (pl. a felhasználói fiókokat a DC kezeli, amelyben a rendszer felhasználóira és adminisztrátoraira vonatkozó XY domain policy biztosítja a jelszóval kapcsolatos elvárásokat)
- Határvédelem (a kapcsolódó követelményeket a határvédelemre vonatkozó pontban definiáljuk), a konfigurációs megvalósítása (például az alábbi tűzfalszabályt alkalmazzuk az eszközön, illetve a rendszer egy biztonsági zónában üzemel, amelyhez az elérés korlátozott. A felépíthető kapcsolatok listája, célja és funkciója a határvédelmi dokumentációban található.)
- Amennyiben külső adatok alapján működik az alrendszer, a külső adatokra vonatkozó bizalmasság- és integritásvédelem is kifejtendő
- Naplózás (a kapcsolódó követelményeket a naplózás pontban definiáljuk): hogyan valósul meg a naplózási rendben meghatározott elvárás

A műszaki dokumentációt elő kell állítani és be kell mutatni a Nemzeti Kommunikációs Hivatalnak.

I.3.1. Rendszerterv

Az informatikai rendszer üzemeltetőinek az akkreditált informatikai rendszer megvalósítása során rendszertervet kell készítenie, amely két részből áll az alábbiakban részletezett tartalommal:

Az első rész tartalmazza:

- a követelmény listát,
- a feldolgozási folyamatok részletes leírását,
- az ellenőrzési rendszer leírását,
- a hibakezelési eljárásokat,
- a rendszer-felügyeleti kapcsolatokat,
- a kapcsolódó rendszerelemek hivatkozását,
- a kapacitástervezési leírást.

A második rész tartalmazza:

- a logikai adatmodellt,
- az I/O adatszerkezeteket,
- a képernyő terveket,
- a lista terveket,
- az infokommunikációs rendszer logikai architektúra ábráját,
- az elemek funkcionális leírását,
- a technikai környezet leírását,

- a biztonsági védelmi funkciók ismertetését.

A rendszertervnek az üzemeltetőnél rendelkezésre kell állnia. Az üzemeltető köteles a Nemzeti Kommunikációs Hivatal arra jogosult munkavállalói, vagy megbízottjai kérésére a rendszertervet bemutatni.

I.3.2. Rendszerbiztonsági terv

Az informatika rendszer üzemeltetőinek rendszerbiztonsági tervet kell kidolgozni, amely

- összhangban áll az üzemeltető szervezeti felépítésével vagy szervezeti szintű architektúrájával;
- meghatározza az akkreditált informatikai rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;
- meghatározza az akkreditált informatikai rendszer működési körülményeit és más akkreditált informatikai rendszerekkel való kapcsolatait;
- a vonatkozó rendszerdokumentáció keretébe foglalja az akkreditált informatikai rendszer biztonsági követelményeit;
- meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés-bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;
- gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
- frissíti a rendszerbiztonsági tervet az akkreditált informatikai rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- elvégzi a szükséges belső egyeztetéseket;
- gondoskodik arról, hogy a rendszerbiztonsági terv arra nem jogosult személyek számára ne legyen megismerhető, módosítható.

Az üzemeltetőnek naprakész nyilvántartással kell rendelkeznie a rendszerkomponensekről, az üzemeltetett rendszerek alapfeladatairól és szolgáltatásairól. A Nemzeti Kommunikációs Hivatal arra jogosult munkavállalói kérésére az üzemeltető köteles bemutatni az előbbieket.

I.3.3. Cselekvési terv

A Nemzeti Kommunikációs Hivatal cselekvési tervet vár el az akkreditált informatikai rendszerrel nyújtott szolgáltatás vonatkozásában.

Az üzemeltetőnek projekttervet (cselekvési tervet) kell készítenie a megvalósítandó szoftver vonatkozásában. Az akkreditált informatikai rendszer bevezetési projekt során a minimálisan elvárt mérföldkövek az alábbiak:

- További extra követelmények egyeztetése
- A futtatáshoz szükséges körülmények ellenőrzése (pl. tűzfal beállítások)
- Tesztverzió beüzemelése, próbaüzem indítása (párhuzamosan használva a jelenleg futó rendszerrel, ha van ilyen)
- Sérülékenység vizsgálat a tesztverzió vonatkozásában
- Tesztverziós tapasztalatok kiértékelése, visszacsatolás a fejlesztéshez
- Éles verzió üzembe állítása, fejlesztői felügyelet biztosítása
- Sérülékenység vizsgálat az éles verzió vonatkozásában
- Éles verziós tapasztalatok kiértékelése, visszacsatolás
- A fejlesztő általi felügyelet megszüntetése, átadási eljárás

A cselekvési tervet a rendszert üzemeltető szervezet vezetője és a rendszergazda által jóvá kell hagyatni. A bevezetési projekt során azonosított koncepcionális hiányosságok javítására, valamint az akkreditált informatikai rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló további cselekvési terveket az üzemeltetőknek szintén jóvá kell hagyatniuk, illetve végre kell hajtaniuk.

I.3.4. Implementáció Terv

Az akkreditált informatikai rendszer követelményspecifikációiban megfogalmazott igények alapján az üzemeltető köteles rögzíteni a telepítési és konfigurációs lépéseket mind a fejlesztett komponensek, mind a kész, ún. „dobozos termék” esetében.

A következőket kell tartalmaznia:

- a rendszer működésének áttekintése,
- implementáció folyamata,
- kiszolgálók telepítési folyamata,
- implementációs végeredmény,
- előfeltételek,
- alkalmazott telepítőkészlet,
- előkészületi lépések,
- implementációs lépések,
- ellenőrző/elfogadási lépések,
- migrációs terv,
- Megrendelői tesztelési terv.

Az implementációs tervet el kell juttatni a Nemzeti Kommunikációs Hivatalhoz.

I.4. Üzletmenet-folytonosságra vonatkozó szabályok

Az üzletmenet-folytonossági eljárásrend célja, hogy biztosítsa az akkreditált informatikai rendszer kritikus szolgáltatásainak folyamatos működését, minimalizálja a nem várt események bekövetkezési valószínűségét, illetve csökkentse a nem várt esemény bekövetkeztekor keletkező károk hatásait és elősegítse az akkreditált informatikai rendszer üzemszerű működésének minél hamarabbi visszaállítását.

Az üzemeltető feladata, hogy az üzletmenet-folytonossági eljárásrendjének megfelelően elkészítse az akkreditált informatikai rendszerére vonatkozó terveket.

I.4.1. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

Az üzemeltető tervet készít az akkreditált informatikai rendszer kiesésére vonatkozóan.

Az Üzletmenet-folytonossági Terv kidolgozásával és alkalmazásával csökkenteni kell a működési tevékenységek félbeszakadásának következményét, valamint meg kell védeni a kritikus folyamatokat a biztonsági események és katasztrófák negatív hatásaitól.

Az üzletmenet-folytonossági tervben meg kell határozni és elő kell írni:

- Az üzemeltető az érvényes követelmények szerint dokumentálja, valamint az informatikai rendszert üzemeltető szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az akkreditált informatikai rendszerekre vonatkozó üzletmenet-folytonossági tervet;
- A minimális szolgáltatások biztosításának (alternatív munkafolyamatok) lehetőségeit, az automatizált folyamatok kézi póteljárásait;
- Az alternatív munkafolyamatokra történő átálláshoz és azok szerinti működéshez szükséges személyi és tárgyi feltételeket, erőforrásokat, felkészülési feladatokat (pl. irodaszerek, jogosultságok, egyéb erőforrások);
- Tájékoztatni kell az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;
- Az infokommunikációs erőforrások dinamikus átcsoportosításának, tartalék egységek beiktatásának a lehetőségét, vagy egy idegen cég eszközeinek igénybe vételére épülő tartalék megoldást, illetve a beüzemelés lépéseit;
- Gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható (a szükséges minimum elve alapján);

- Meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
- Rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;
- Jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;
- Fenntartja az informatikai rendszert üzemeltető szervezet által előzetesen meghatározott alapszolgáltatásokat, még az akkreditált informatikai rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
- Kidolgozza a végleges, teljes akkreditált informatikai rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket;
- A tervek tárolási felelőseit és helyszíneit, a tervek frissítése során a legfrissebb verzió valamennyi tárolási helyszínen történő frissítését;
- A katasztrófa-elhárítás előfeltételeként elvégzendő mentések rendszerét.

A kidolgozott tervek alapján rendszeres időközönként teszt jelleggel dokumentált módon rendszer visszaállításokat kell végezni, ami biztosítja a naprakészség ellenőrzését. A visszaállítási tesztek elvégzése az üzemeltető felelőssége.

I.4.2. Az üzletmenet folytonosságának tervezése

Az üzletmenet-folytonosság tervezés keretrendszerének kötelező tartalmi elemei az alábbiak:

- A tervek életbe léptetésének a feltételei, amelyekben rögzíteni kell a követendő folyamatot (észlelés, értékelés, eszkaláció, stb.); – összhangban a Biztonsági események kezelése Tervvel (IR);
- A tervnek tartalmaznia kell az informatikai rendszert üzemeltető szervezeten belüli és kívüli értesítendők listáját – elérhetőségekkel (pl. szállítókkal, partnerekkel, hatóságokkal – pl. rendőrség, tűzoltóság, önkormányzat – történő kapcsolatfelvétel) – összhangban a Biztonsági események kezelése Tervvel (IR);
- A szervezeten belül és kívül alkalmazandó kommunikációs feladatokat; (pl. a nyilvánosság, médiák kezelésére);
- Az üzleti területek által alkalmazandó részletes alternatív munkafolyamat;
- Az informatikai területek alternatív munkafolyamatokat támogató feladatai;
- Újraindítási eljárás feladatai;
- Karbantartási terv, amelyben a terv tesztelésének módja és időpontja, és a terv karbantartásának eljárása szerepel;
- Oktatási és tudatosítási tevékenységek;
- A terv egyes feladatainak végrehajtásáért felelős személyek;
- A tervek tárolásának helyszínei és azok egységes frissítésének menete.

A fentiek elkészítése az üzemeltető feladata az akkreditált informatikai rendszer vonatkozásában.

I.4.3. Az üzletmenet-folytonosságra vonatkozó tervek karbantartása

Az üzletmenet-folytonossági tesztelés céljai:

- A terv aktualitásának, alkalmazhatóságának ellenőrzése;
- A terv hibáinak felderítése;
- Meggyőződés a visszaállítási dokumentumok elérhetőségéről;
- Az érintettek megismertetése a feladataikkal és gyakorlati képzésük.

Az üzletmenet-folytonossági tervek tesztelési terve a terv egyes elemei tesztelésének módját és időpontját tartalmazza. A tesztelési terveket az üzemeltetőnek kell elkészítenie.

A tesztek tapasztalatait ki kell értékelni és azok eredménye alapján (szükség estén) aktualizálni kell az üzletmenet-folytonossági tervet. Az üzemeltetőnek legalább egy tesztet kell futtatnia és a tanulságok alapján legalább egyszer frissítenie kell az üzletmenet-folytonossági tervet.

Az üzleti területek által alkalmazandó alternatív munkafolyamatot az üzleti területeknek évente legalább egy alkalommal szimulációs teszt keretein belül kell tesztelni, az informatika szükséges mélységű bevonásával. A

szimulációs teszt során a felelősök előre kidolgozott forgatókönyv alapján, annak egyes lépéseit végrehajtva győződnek meg a terv működőképességéről.
Az üzleti területek által alkalmazandó alternatív munkafolyamat kialakításáért, teszteléséért és frissítéséért az érintett üzleti terület a felelős.
Az akkreditált informatikai rendszer újraindítását az informatikának félévente kell tesztelnie az üzleti területek szükséges mélységű bevonásával.
Az akkreditált informatikai rendszer újraindítási folyamatának, illetve az üzletmenet-folytonossági terv informatikai részeinek kialakításáért, teszteléséért és frissítéséért, a rendszer üzemeltetője a felelős.
A terveket frissíteni kell az új berendezések beszerzése, az operációs rendszer frissítése esetében, vagy, ha változások következnek be:

- a személyzetben,
- a címekben, telefonszámokban,
- az üzleti- és informatikai stratégiában,
- a helyszínekben, segédprogramokban, és erőforrásokban,
- a jogszabályokban,
- belső szabályzatokban
- a szerződő felek, szolgáltatók, vagy fontos ügyfelek tekintetében,
- a kockázatban (működési és pénzügyi),

Frissíteni kell a terveket továbbá a tervek tesztelését követő kiértékelések alapján.
A frissített üzletmenet-folytonossági terv új verzióját valamennyi tárolási helyszínre teríteni és aktualizálni kell.

I.4.4. Az akkreditált informatikai rendszer helyreállítása és újraindítása

Az Üzletmenet-folytonossági tervnek pontosan kidolgozott utasításokat kell tartalmazni arra, hogy egy, a számítógéptermet érintő katasztrófa esetén milyen lépések után állítható helyre a normális vagy a csökkentett kapacitású működés.
Az Üzletmenet-folytonossági tervnek a bekövetkezett katasztrófára és a helyreállításra vonatkozóan a következőket kell tartalmaznia:

- Katasztrófát követő helyreállítandó célállapot;
- A katasztrófa események definíciója;
- A katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;
- A katasztrófa terv hatóköre;
- A megelőzés érdekében végzett tevékenységeket;
- Felkészülés a katasztrófa elhárítására;
- Katasztrófa esetén végrehajtandó tevékenységek;
- A helyreállítási terv tesztelése, karbantartása.

A fenti pontokat az üzemeltetőnek kell definiálnia.
A tevékenységeket az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) rendszeresen ellenőriznie kell.
A katasztrófa kezelésére és a helyreállításra vonatkozó előírásokat minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új nagyteljesítményű hardverelemek változása).
A rendszergazdának – mindezeken túl – gondoskodnia kell az akkreditált informatikai rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.
A rendszer helyreállítási és újraindítási tervnek (DRP) olyan szintű technikai részletezettséggel kell rendelkeznie, mely alapján egy, az informatikai rendszert üzemeltető szervezeten kívüli, megfelelő informatikai rendszerüzemeltetési ismeretekkel rendelkező szakember (a szükséges jogosultságok birtokában) a rendszer (szolgáltatás) helyreállítását maradéktalanul el tudja végezni.

A számítógépteremben működő akkreditált informatikai rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot (DRP) a rendszergazda állítja össze, és az Információbiztonsági Felelős (IBF) hagyja jóvá. A dokumentum egy példányát a számítógépteremben kell tárolni.
A DRP első verziójának elkészítéséért az üzemeltető a felelős.

I.4.5. A folyamatos működésre felkészítés

Az üzletmenet-folytonosság megfelelő szinten tartása, valamint a nem várt esemény esetén alkalmazandó eljárások megfelelő hatékonysággal történő végrehajtása érdekében az üzletmenet-folytonosság biztosításában részt vevők részére felkészítő és ismétlő képzéseket kell tartani. Az akkreditált informatikai rendszer vonatkozásában az üzletmenet-folytonossági képzések végrehajtásáért az üzemeltető felel.
A képzéseken a következő területeket kell minimálisan érinteni:

- Az akkreditált informatikai rendszerre ható főbb fenyegetések;
- A fenyegetések minimalizálása érdekében megtett kockázatkezelő intézkedések;
- A konfigurációkezelési eljárások megfelelő használata;
- A változáskezelési eljárások megfelelő használata;
- A mentési eljárások;
- A katasztrófa esetén szükséges lépések, riadólánc;

A képzés tartalmának összeállítása és a képzések megtartása az üzemeltető feladata.

I.4.6. Rendszerkövetés (támogatás)

Az akkreditált informatikai rendszerhez a rendszer üzemeltetőjének szerződésben rögzített feltételek mellett az alábbi területeket magába foglaló támogatást kell nyújtania:

- az infokommunikációs rendszerben felmerülő hibák javítása,
- a Nemzeti Kommunikációs Hivatal fejlesztési igényeinek ellátása,
- az infokommunikációs rendszer futtató környezetének (operációs rendszer, adatbázis rendszerek) frissítése.

A szerződésben rögzíteni kell a támogatás körülményeit (határidők, rendelkezésre állás, helyszíni vagy telefonos támogatás) is a megfelelő szolgáltatási szint biztosítására. A paraméterek pontos értékének meghatározása az infokommunikációs rendszer adatgazdájának és az informatikai üzemeltetésért felelős vezető feladata.

I.4.7. Rendszerintegritás

Fejlesztett komponensek esetében a szerződésben rögzíteni kell, hogy a megvalósított szoftver megfelelően biztonságos környezetben, kontrollált körülmények között készült, így nem tartalmaz kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan a Nemzeti Kommunikációs Hivatalnak vagy bármelyik más felhasználónak bármilyen kára keletkeznek, akkor azért az üzemeltető teljes és korlátlan anyagi felelősséggel tartozik.

I.5. Rendszer és szolgáltatás beszerzés

Az üzemeltető feladata gondoskodni arról, hogy az akkreditált informatikai rendszer és szolgáltatás kapcsán meghatározott eljárásrendben megfogalmazott követelmények a fejlesztett rendszer kapcsán teljesüljenek.

I.5.1. A rendszer fejlesztési életciklusa

Az üzemeltető teszt- és éles verzió előállítására köteles.
Az akkreditált informatikai rendszer teljes életútján, annak minden életciklusában az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) figyelemmel kíséri az informatikai biztonsági helyzetet. A fejlesztések életciklusainak egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint az informatikai rendszert üzemeltető szervezetre vonatkozóan meghatározza az információbiztonsági szerepköröket betöltő személyeket.

Az informatikai rendszert üzemeltető szervezet számára minimálisan az alábbi információ biztonsági szerepkörök meghatározására kötelezett:

- Információbiztonsági Felelős (IBF)
- Rendszergazda

Az akkreditált informatikai rendszerére vonatkozóan az alábbi életciklus szakaszokat határozza meg:

- követelmény meghatározás
- fejlesztés vagy beszerzés
- megvalósítás vagy értékelés
- üzemeltetés és fenntartás
- kivonás (archiválás, megsemmisítés)

A Nemzeti Kommunikációs Hivatal külső és belső ellenőrzési eszközökkel ellenőrizheti, hogy a külső akkreditált informatikai rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

A rendszert üzemeltető szolgáltatónak a szerződés alapján lehetővé kell tennie a támasztott követelmények (pl. környezeti feltételek, személyi biztonság, logikai feltételek) ellenőrzését a Nemzeti Kommunikációs Hivatal, vagy annak megbízottja számára.

I.5.2. Funkciók, portok, protokollok, szolgáltatások

A Nemzeti Kommunikációs Hivatal megköveteli, hogy az akkreditált informatikai rendszert üzemeltető szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat. A számítógépes hálózat határvédelmi eszközeit az üzemeltetőnek úgy kell beállítani, hogy csak a szükséges portok legyenek elérhetőek.

II. Felhasználói szerepkörökkel és felhasználói jogosultsági szintekkel kapcsolatos követelmények

Az első alfejezet az MK rendeletben a felhasználói szerepkörökkel és felhasználói jogosultsági szintekkel kapcsolatos tételesen meghatározott követelmények részletezését tartalmazza. A további alfejezetek pedig a követelményekhez kapcsolódó részletesebb biztonsági és funkcionális elvárásokat írják le.

II.1. A jogszabályi elvárásokkal kapcsolatos követelmények

Az MK rendelet 5. § értelmében az informatikai rendszernek elkülönítetten kell kezelnie a Hivatal, az Érintett szervezet és a Szállító szerepköreit. Az egyes szerepkörökön belül elkülönítetten kell kezelni az adminisztrátori, az engedélyező és a felhasználói jogosultsági szinteket.

Az MK rendelet 6. § szerint a Hivatal rendelkezik felhasználói, engedélyező és adminisztrátor jogosultságokkal. Az érintett szervezet és a szállító felhasználói szerepkörrel rendelkezik.

Az informatikai rendszernek elkülönítetten kell kezelnie a Nemzeti Kommunikációs Hivatal, az Érintett szervezetek és a Szállítók szerepköreit. Kezdetben csak ezek a szerepkörök szükségesek. A későbbiekben azonban előfordulhat a szerepkörök számának bővítése a felhasználási tapasztalatok alapján, ezért a rendszernek rugalmasan, bővíthető módon kell a szerepköröket kezelnie.
Az egyes szerepkörökön belül elkülönítetten kell kezelni az engedélyező, az adminisztrátor és a felhasználói jogosultsági szinteket. A jogosultsági szintek rendszere kezdetben csak ezen a három szinten elvárt. A későbbiekben azonban várható a jogosultsági szintek bővítése, ezért a rendszernek rugalmasan, bővíthető módon kell a jogosultsági szinteket kezelnie.
Az Érintett szervezetek és a Szállítók felhasználói csak felhasználói szerepkörrel rendelkeznek. A Nemzeti Kommunikációs Hivatal rendelkezik felhasználói, engedélyező és adminisztrátor jogosultságokkal is.
A fentieken túl kezelni kell a rendszergazda szerepkört is, ami a rendszer üzemeltetésével, felügyeletével és egyéb rendszergazdai feladatokkal kapcsolatos.

Az egyes külső szerepkörökhöz tartozó funkciók és korlátozások az alábbiak:

- Érintett szervezet felhasználó: csak a saját szervezetéhez kapcsolódó beszerzések adatait láthatja és kezelheti (létrehozás, módosítás, törlés). Más szervezet által kezelt adatokhoz nem férhet hozzá. Minden adat módosítása naplózott formában történik. Az Érintett szervezet a hozzá tartozó beszerzések Szállítóinak az adataiból csak a beszerzéshez kapcsolódó adatokat láthatja. Szűréseket, listákat csak a saját szervezetéhez tartozó beszerzésekről gyűjthet le. Az Érintett szervezetnek több felhasználói fiókja is lehet, ezek között az adatokhoz történő hozzáférésben nincs különbség.
- Szállító felhasználó: csak a saját cégéhez kapcsolódó beszerzések adatait láthatja és kezelheti (létrehozás, módosítás, törlés). Más szállító által kezelt adatokhoz nem férhet hozzá. Minden adat módosítása naplózott formában történik. A Szállító a hozzá tartozó beszerzések megrendelőinek (Érintett szervezetek) adataiból csak a beszerzéshez kapcsolódó adatokat láthatja. Szűréseket, listákat csak a saját cégéhez tartozó beszerzésekről gyűjthet le. A Szállítónak több felhasználói fiókja is lehet, ezek között az adatokhoz történő hozzáférésben nincs különbség.
- NKOH: Az NKOH fiókok általános elvként minden Érintett szervezet, Szállító és Beszerzés adataihoz hozzáféréssel rendelkeznek. Az egyes jogosultsági szintek határozzák meg, hogy a hozzáférések miben különböznek egymástól. Az NKOH szerepkör megtekintheti, leszűrheti az egyes Érintett szereplők, Szállítók és Beszerzések adatait. A szerepkör által biztosítandó adatok beviteli és megtekintési funkcióihoz fér hozzá, továbbá joga van az egyes beszerzésekhez tartozó tételek egyenkénti jóváhagyására (amennyiben az jóváhagyást igényel) vagy tiltására. A szerepkör által biztosítandó engedélyeztetési folyamatokhoz és adatbeviteli funkciókhoz fér hozzá. Lekérheti a rendszer által kezelt kimutatásokat, riportokat. Jogosultsága van meghatározni, hogy az egyes beszerzések jóváhagyás kötelesek legyenek-e vagy sem.

A Hivatal, mint szerepkör az informatikai rendszerben előállt Beszerzések adataihoz hozzáfér, függetlenül a Beszerzések aktuális életciklus állapotától. Az Érintett szervezet, mint szerepkör csak az általa kezdeményezett Beszerzések adataihoz fér hozzá, függetlenül a Beszerzések aktuális életciklus állapotától. A Szállító, mint szerepkör csak az általa kezelt Beszerzések adataihoz fér hozzá, függetlenül annak életciklus állapotától.

Funkcionális követelmények szerepkörök szerint

1. Hivatal
    a. Nyomon követheti a Beszerzések végrehajtását, illetve adatokat érhet el a Beszerzésekről
2. Érintett szervezet
    a. Megtekintheti a Portál rendszerekből átvett beszerzéssel kapcsolatos adatokat.
    b. Feltöltheti és módosíthatja a beszerzéssel kapcsolatos további adatokat.
    c. A Beszerzéssel kapcsolatos, a Szállító által összeállított, tervsorokból álló tervet megtekintheti, a tervet elfogadhatja.
    d. Elfogadhatja a Teljesítésigazolásokat
    e. Megtekintheti a Számlákat
3. Szállító
    a. Összeállítja a Beszerzés tervét, feltölti a terv sorait, szükség esetén tervmódosítást hajt végre.
    b. Rögzíti az elfogadásra váró teljesítési igazolások adatait és opcionálisan feltölti a Teljesítésigazolás adatait és adott esetben, ha a rendszer kezeli, a kapcsolódó dokumentumo(ka)t.
    c. Rögzíti az elfogadott Teljesítésigazolásokra hivatkozó Számla adatait, és ha a rendszer kezei, opcionálisan feltölti a Számlát és adott esetben egyéb kapcsolódó dokumentumo(ka)t.

Az egyes későbbi fejezetek a fenti elvárásokat tovább részletezhetik még.

II.2. Azonosítás és hitelesítés

A rendszer jellegét tekintve kétféle felhasználói fiókot kezel, és ezen belül további típusokat:

- belső, a rendszer működtetéséért és felügyeletéért felelős felhasználói fiókok (privilegizált fiókok)
- külső, az operatív munkavégzésért felelős felhasználói fiókok (a Nemzeti Kommunikációs Hivatal felhasználó a háromféle – felhasználói, engedélyező és adminisztrátor – jogosultsági szintben, az érintett szervezetek „felhasználó” jogosultsági szinten, a szállítók „felhasználó” jogosultsági szinten)

A „belső” és a „külső” jelzőket az üzemeltető szemszögéből kell értelmezni. Mivel a belső és a külső felhasználói fiókok rendszerbeli szerepe és a jogosultságainak kiosztása és kezelése is teljesen más, külön alfejezetekben írunk mindegyikről.

A belső felhasználók szerepe a rendszer üzemeltetése. Ők rendelkeznek olyan szintű hozzáféréssel a rendszerhez, ami minden rendszerelemet és adatot is érint. Az ő jogosultságaikat a rendszer-üzemeltető cég belső szabályzatainak kell kezelniük (ki mihez fér hozzá, stb.).

A külső felhasználók viszont csak egy kontrollált felületen férnek hozzá az adatokhoz, a rendszer elemeit nem tudják módosítani (sem a konfigurációt, sem a szoftver komponenseket). Az üzemeltető a külső felhasználók szervezeteivel, cégeivel kötött szerződések alapján adja ki, és kezeli a kapcsolódó jogosultságokat. A jóváhagyási folyamat a szerződés része kell, hogy legyen. A megkötött szerződésben definiált a felhasználók és azok jogosultságainak kezelése.

II.2.1. Azonosítási és hitelesítési eljárásrend

Az akkreditált informatikai rendszerhez történő hozzáférés során a hozzáférők megfelelő szintű azonosítása és hitelesítése érdekében az üzemeltető feladata az, hogy a kifejlesztett akkreditált informatikai rendszer azonosítási és hitelesítési eljárását az implementáció előtt pontosan dokumentálja. Az akkreditált informatikai rendszer azonosítási és hitelesítési metódusait az előzetesen jóváhagyott dokumentumban szereplő módon kell megvalósítani.

A jelszavak tárolása csak a kriptográfiai védelem pontban leírt módon lehetséges.

II.2.2. Azonosítás és hitelesítés

Az akkreditált informatikai rendszernek egyedileg kell azonosítania és hitelesítenie a Nemzeti Kommunikációs Hivatal, az érintett további szervezetek és a szállítók valamennyi felhasználóját és a felhasználók által végzett tevékenységeket. Ezért nem elfogadható a csoportos azonosítók alkalmazása. Minden felhasználót (legyen az bármelyik szerepkör tagja is) egyedi azonosítóval kell felruházni.
Ennek érdekében az üzemeltető kapcsolódó dokumentációjában meghatározott névkonvenció alapján egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

II.2.3. Hálózati hozzáférés privilegizált (belső) fiókokhoz

Az akkreditált informatikai rendszerekhez történő privilegizált (rendszergazdai) hálózati hozzáférésre legalább kéttényezős azonosító mechanizmust kell megvalósítani. A többtényezős autentikáció egyik eleme a jelszó, a másik elem lehet:

1. piaci hitelesítés szolgáltatótól beszerzett chipkártya,
2. szoftveres kulcs,
3. egyszeri jelszógenerátorral előállított jelszó (One-Time Password – OTP),
4. Egyéb, birtoklás alapú azonosítási és hitelesítési megoldás (pl. tenyérértérkép, retina).

A kétfaktoros autentikáció második tényezőjére vonatkozóan, az implementáció előtt, az üzemeltető kötelessége javaslatot adni.

II.2.4. Azonosító kezelés

Az akkreditált informatikai rendszerben az azonosítókat az üzemeltető rendszergazdái kezelik. A fejlesztett akkreditált informatikai rendszernek alkalmazkodnia kell a belső szabályokhoz. Az azonosítók létrehozásakor törekedni kell arra, hogy az azonosítók egyértelműen hozzá legyenek rendelve a kívánt egyénhez, csoporthoz vagy eszközhöz. Az üzemeltető felelőssége, hogy előzetesen oktassa a rendszergazdákat az alkalmazandó szabályok vonatkozásában, illetve az átadási folyamat során tájékoztassa a rendszergazdákat, hogy a későbbiekben önállóan végezhessék el a kifejlesztett rendszerazonosító kezeléshez kapcsolódó feladatokat.
Az azonosítókat úgy kell létrehozni, hogy a rendszer egy évnyi inaktivitás után tiltsa le a nem használt azonosítókat. Az azonosítók törlésére ne legyen lehetőség, azonban lehetőséget kell biztosítani a nem használt azonosítókat inaktív állapotba állítására.
Az azonosítók ismételt felhasználása tiltott, ezért a szoftverben biztosítani kell, hogy korábbi azonosítót ne oszthassanak ki ismételten. Az ismételten aktivizált (azonos személyhez rendelt) azonosítók nem tartoznak a tiltás hatálya alá.

II.2.5. A hitelesítésre szolgáló eszközök kezelése

A hitelesítésre szolgáló eszközök (továbbiakban: a jelszavak, de ide tartoznak a birtoklás alapú hitelesítő-eszközök is) a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.
Az akkreditált informatikai rendszerben csak olyan megoldások használhatóak, amelyek jelszókezelő alrendszere:

- lehetővé teszi a felhasználók számára jelszavuk kiválasztását és megváltoztatását;
- kikényszeríti az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor, vagy lehetővé teszi a felhasználók számára a kezdeti jelszavuk közvetlen megadását;
- kikényszeríti a megfelelő minőségű jelszavak használatát (erre vonatkozóan a következő pontok adnak útmutatást);
- kikényszeríti a rendszeres jelszóváltoztatást;
- megtiltja a korábban használt jelszavak ismételt felhasználását;

- beíráskor nem jeleníti meg a jelszavakat a képernyőn (maszkolás);
- a jelszó állományokat rejtjelezve tárolja (lásd a Kriptográfiai védelem pontot);
- támogatja a szállító alapértelmezett (pl. rendszergazda) jelszavának megváltoztatását a szoftver installálása után. Ennek végrehajtása a rendszergazda feladata.

Az üzemeltető kötelessége gondoskodni arról, hogy a kifejlesztett rendszer minden fenti követelménynek megfeleljen.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell műszaki megoldással kikényszeríteni:

- a jelszó legalább nyolc karakter hosszú legyen;
- a jelszó tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;
- a jelszavakat 60 naponta meg kell változtatni;
- a jelszavakat két napon belül nem szabad megváltoztatni;
- a felhasználó utolsó 10 jelszava nem adható meg újra;

Az üzemeltető felelőssége, hogy a megvalósított szoftverben a fenti szabályok ki legyenek kényszerítve.

Az akkreditált informatikai rendszerben a jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni, úgy, hogy:

- a felhasználók az Informatikai Biztonsági Szabályzat megismeréséről szóló nyilatkozat aláírásával, elfogadásával kötelezik magukat arra, hogy vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;
- biztosítani kell, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra;
- hibás belépési kísérletekből adódó zárolás esetén előre beállított időtartam (5 perc) eltelte után engedélyezze vissza a felhasználói fiókot.

Az üzemeltető felelőssége, hogy a fenti szabályokat megfelelő műszaki megoldásokkal kényszerítse ki a kifejlesztett rendszerben. Nem tehető semmilyen jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre, vagy tárolásra; az üzemeltető felelőssége, hogy ne is kerüljön a fejlesztési folyamat során.

Az akkreditált informatikai rendszerhez történő hozzáférés során alkalmazott jelszavak idegen kézbe kerülése, illetve a jelszószabályok be nem tartása biztonsági incidensnek minősül, ezért ezekben az esetekben azonnal értesíteni kell az üzemeltető szervezet Információbiztonsági Felelősét (IBF).

II.2.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az akkreditált informatikai rendszerben alkalmazott hitelesítésre szolgáló eszköz hibás azonosító vagy jelszó megadása esetén csak olyan hibaüzenetet adhat vissza, amelyből nem szerezhető további információ sem az azonosító, sem a jelszó összetételéről.

Ezért az üzemeltető felelőssége, hogy a kifejlesztett szoftver csak egyfajta visszajelzést adhat hibás autentikáció esetén: „A megadott felhasználói azonosító, vagy jelszó hibás”. Akár a felhasználói azonosító volt hibás, akár a jelszó, csak az idézett szövegnek szabad megjelennie a képernyőn.

II.2.7. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az akkreditált informatikai rendszer célja a közbeszerzések végrehajtásának és ellenőrzésének informatikai támogatása. Ezért várhatóan sok külső (az üzemeltető szervezetén kívüli) felhasználó jelenlétére számíthatunk.

A külsős felhasználók akkreditált informatikai rendszerhez történő hozzáférése során (a belsős felhasználókhoz hasonlóan) egyedi azonosítókat kell létrehozni. A szervezeten belüli és szervezeten kívüli felhasználók között nem szükséges különbséget tenni.

II.3. Hozzáférés ellenőrzése

II.3.1. Hozzáférés ellenőrzési eljárásrend

Az akkreditált informatikai rendszer rendszerkomponenseihez, adataihoz, az informatikai- és adatvagyonához való hozzáférést, a hozzáférés kezelését az üzemeltető saját eljárásrendjében foglaltak szerint kell kezelni. Az üzemeltető felelőssége, hogy

- a rendszer bevezetésekor egyeztesse és hagyassa jóvá a hozzáférési jogosultsági szintek (fióktípusok, szerepkörök) rendszerét,
- a projekt közepére hozza létre a Nemzeti Kommunikációs Hivatal, az Érintett szervezetek, a Szállítók és partnereinek személyi állományi vonatkozásában az érintett munkavállalók azonosítóit a jóváhagyott jogosultsági szintekhez kötve,
- a projekt végére pedig tanítsa meg a rendszergazdát, hogy miként lehet meglévő, vagy új felhasználói azonosítót szerepkörhöz rendelni, fióktípust módosítani.

A hozzáférés ellenőrzési eljárásrendet természetesen a bevezetési projekt vége után is alkalmazni kell.

II.3.2. Felhasználói fiókok kezelése

Az akkreditált informatikai rendszerében a következőkben leírtak szerint kell a felhasználói fiókokat kezelni.

II.3.2.1. Fióktípusok

Az akkreditált informatikai rendszerhez történő hozzáférés érdekében a rendszerdokumentációban a következő fióktípusok kerültek létrehozásra:

- felhasználó (külső felhasználói fiók),
- engedélyező (külső felhasználói fiók),
- adminisztrátor (külső felhasználói fiók),
- rendszergazda (belső felhasználói fiók)

A külső felhasználói fiókokat a rendszergazdák, a rendszergazda fiókokat az informatikai terület vezetője kezeli. Az akkreditált informatikai rendszerben a rendszergazdai fiókok száma véges, a legtöbb felhasználó az első három kategória valamelyikébe fog tartozni.

II.3.2.2. Csoportok

Az akkreditált informatikai rendszernek külön kell kezelnie a Nemzeti Kommunikációs Hivatalhoz tartozó (külső) felhasználói fiókokat (pl. NKoH csoportnéven), az Érintett szervezetek felhasználói fiókjait (utalva az Érintett szervezet nevére), illetve a Szállítókhoz rendelt felhasználói fiókokat (utalva a Szállító nevére).
További csoportok létrehozásának lehetőségét kell biztosítani szükséges esetén minden közbeszerzési eljárás vonatkozásában. A csoportba azokat a fiókokat kell bevonni, akik részt vesznek a kapcsolódó projektben. A csoporttagságok karbantartása a rendszergazdák feladata. Már létrehozott csoportokat nem kell törölni.
A belső felhasználók vonatkozásában a csoportok kialakításáról az üzemeltető önállóan is dönthet.

II.3.2.3. Szerepkörök

Az akkreditált informatikai rendszerében a feladatellátástól függően a következő külső szerepkörök kerüljenek kialakításra:

- engedélyező,
- adminisztrátor,
- felhasználó

A Nemzeti Kommunikációs Hivatal munkavállalói mindhárom szerepkört betölthetik, ám az Érintett szervezetek és Szállítók csak „felhasználó” szerepkörű fiókokat kérhetnek maguknak.

II.3.2.4. Tagsági feltételek

A külső felhasználók és szerepkörük meghatározása az informatikai rendszer üzemeltetőjének szerződésében rögzített módon kell történnie.
A belső (üzemeltetői) szerepkörök tagsági feltételeit a munkatársak munkaköri leírása alapján kell kialakítani.

II.3.2.5. Hozzáférési jogok igénylése

Az akkreditált informatikai rendszeréhez történő új hozzáférést, meglévő hozzáférési jog módosítását, illetve hozzáférési jog visszavonását a jelen fejezetben leírt eljárásrend alapján kell kezelni.

II.3.2.6. Az új hozzáférés igénylési folyamat leírása belső (privilegizált) felhasználói fiókok esetén

Az üzemeltető önállóan határozhatja meg a belső felhasználói fiókok hozzáférési folyamatát. Az egyetlen követelmény, hogy a folyamat visszakereshető legyen. Az üzemeltető, mint jogi személy, teljes felelősséggel tartozik a jogosulatlan privilegizált fiókok létrehozásából adódó anyagi károkért.

II.3.2.7. Az új hozzáférés igénylési folyamat leírása külső felhasználói fiókok esetén

A hozzáférési jogok igénylése az igénylő szervezet (Nemzeti Kommunikációs Hivatal, vagy az Érintett szervezet, vagy a Szállító) és az üzemeltető között kötött szerződésben rögzített módon történik. A szerződés megkötésekor a felhasználói fiókokra feladott kezdeti igény az erre szolgáló szerződésmelléklet kitöltésével kezdeményezhető. Az igényben meg kell jelölni a jogosultság szintjét (szerepkört), illetve azt az időszakot, amelyre a jogosultságot biztosítani kell.

A feladott igények jóváhagyási metódusát a szerződésben kell rögzíteni. A jóváhagyó igazolja, hogy a feladatellátáshoz szükséges a jogosultság biztosítása. A jóváhagyás a ticketing rendszerben történik.

Az igényt ezt követően továbbítani kell az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) részére, aki jóváhagyja a jogosultságigénylést a ticketing rendszerben.

A jóváhagyott jogosultságigénylést ezt követően el kell küldeni a rendszergazdák részére, akik intézkednek a jogosultság kiadásáról.

A rendszergazda rögzíti a fióklétrehozás kezdetét a ticketing rendszerben.

A rendszergazda az igényelt beállításokkal létrehozott felhasználói fiókról telefonon vagy személyesen értesíti az igénylőt, és megadja a belépéshez használatos felhasználói nevet, az első belépést lehetővé tevő kezdeti jelszót és szükség esetén egyéb fontos adatokat.

A kért feladatok elvégzésének bizonylatolása érdekében a rendszergazda e-mailben tájékoztatja az igénylőt és a jóváhagyót a jogosultságok megadásáról és a felhasználónévről, valamint a ticketing rendszerben dokumentálja a felhasználói fiókhoz tartozó jogosultságok változását. A rendszergazda ezt követően lezárja a fióklétrehozás folyamatát a ticketing rendszerben.

A tárolt, jóváhagyott igények a ticketing rendszerben kerülnek megőrzésre.

Az üzemeltetésért felelős szervezet Információbiztonsági Felelőse (IBF) a ticketing rendszer által tárolt jóváhagyási folyamatokat és a ténylegesen kiadott jogosultságokat bármikor összevetheti és ellenőrizheti. Az esetlegesen feltárt anomáliákról az üzemeltetőt azonnal értesíti.

II.3.2.8. Hozzáférési jog módosítása, csoporttagság létrehozása

A hozzáférési jog változtatásában érintett dolgozó vezetője a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához az előző pontban leírt módon, a szerződésben rögzített folyamat szerint jár el.

A módosítások dokumentálására a ticketing rendszer bejegyzései használandók.

II.3.2.9. Hozzáférési jog visszavonása

Az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) és minden szerződött szervezetnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a ticketing rendszerben kell kezdeményezni. Az üzemeltető és az Érintett szervezet között lévő szerződésben meghatározott módon kell végig vinni a folyamatot (jóváhagyás).

A jóváhagyott igényt a ticketing rendszer továbbítja az üzemeltető szervezet rendszergazdájának, aki intézkedik a jogosultság visszavonásáról.

A rendszergazda rögzíti a hozzáférési jogosultság visszavonás megkezdésének tényét a ticketing rendszerben.

A rendszergazda visszavonja a jogosultságot.

A rendszergazda e-mail-en tájékoztatja a munkahelyi vezetőt és a jóváhagyót a visszavonás tényéről és a ticketing rendszerben lezárja a jogosultság visszavonási folyamatot.

II.3.2.10. Felhasználói fiókok felülvizsgálata

A felhasználói hozzáféréseket, jogosultságokat a rendszergazda a rendszer adatgazdájával bármikor felülvizsgálhatja.

A felhasználói fiókok kezelését, illetve a rendszeres felülvizsgálatok megfelelőségét évente az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF-je) ellenőrzi az érvényes hozzáférési engedélyek alapján, a következő metódus szerint:

Minden év január 31-e előtt lekérdezi a rendszerben lévő felhasználókat és minden Érintett szervezetnek, valamint Szállítónak és a Nemzeti Kommunikációs Hivatalnak is elküldi a jelenleg aktív felhasználók listáját. Az Érintett szervezeteknek ellenőrizniük kell, hogy a listán szereplő felhasználók valóban aktív státuszúak-e a szervezetnél. Amennyiben eltérést tapasztalnak, azt kötelesek azonnal jelenteni az üzemeltető szervezet Információbiztonsági Felelősének (IBF). Amennyiben nem tapasztalnak eltérést, a kapott listán fel kell tüntetniük ennek tényét és hivatalos aláírással ellátva el kell küldeniük az üzemeltető szervezet Információbiztonsági Felelősének (IBF).

Eltérés esetén az üzemeltető azonnal tájékoztatást kap. Eltérés esetén az üzemeltető haladéktalanul köteles a szoftverben a hibát felderíteni és javítani. Amennyiben nincs eltérés, az üzemeltető nyilatkozatot kap erről. A nyilatkozatok eredetijét az üzemeltető felelőssége gyűjteni.

II.3.3. Hozzáférés ellenőrzés érvényesítése

Az akkreditált informatikai rendszert fel kell készíteni a jelen eljárásrendben foglalt hozzáférés-ellenőrzési követelmények alapján a hozzáférések érvényre juttatására.

II.3.4. Sikertelen bejelentkezési kísérletek

Az akkreditált informatikai rendszernek a következő fiókzárolási házirendet kell alkalmaznia sikertelen bejelentkezési kísérletek esetén:

1. táblázat: Fiókok zárolásával kapcsolatban követendő szabályok

Szabály megnevezése	Beállított érték
Fiókzárolási küszöb	5 sikertelen próbálkozás
Fiókzárolás időtartama	5 perc
Fiókzárolási számláló nullázása	5 perc

A rendszergazdát csak indokolt esetben szabad bevonni a fiókzárolás feloldására.

II.3.5. A rendszerhasználat jelzése

Az akkreditált informatikai rendszerhez való hozzáférés előtt – még az azonosítási és hitelesítési folyamat megkezdése előtt – tájékoztatni kell a felhasználókat a következőkről:

- a rendszerhasználatot a Hivatal figyeli, rögzíti, naplózza;
- a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgári jogi felelősségre vonással jár;
- a rendszer használatával a felhasználó elfogadja és tudomásul veszi a fentieket;
- A képernyőn lehetőséget kell biztosítani (egy klikkelhető link formájában), hogy a felhasználó tudomást szerezzen minden olyan dokumentumról, amely szabályzóként releváns az akkreditált informatikai rendszer vonatkozásában.

A figyelmeztető üzenetet mindaddig a képernyőn kell tartani, amíg a felhasználó közvetlen műveletet nem végez a rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

II.3.6. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az akkreditált informatikai rendszerben nem engedélyezettek az azonosítás és hitelesítés nélkül végzett tevékenységek.

II.3.7. Távoli hozzáférés

Az akkreditált informatikai rendszerhez engedélyezett a távoli hozzáférés. Távoli hozzáférés kizárólag HTTPS kapcsolat (SSL/TLS felett) segítségével lehetséges. Titkosítatlan (HTTP) forgalom nem engedélyezhető. Az SSL/TLS kapcsolat kötelező paramétereit,kriptográfiai előírásait a Kriptográfiai védelem pont részletezi. A kapcsolódási pontok egyelőre nem korlátozódnak rögzített IP tartományokhoz. Az akkreditált informatikai rendszerhez kapcsolódók vonatkozásában korlátozást nem kell alkalmazni. Amennyiben a későbbiekben felmerül korlátozási igény, akkor az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) bevonásával ki kell dolgozni annak technikai megvalósítását, a felhasználás feltételeit, korlátait és az engedélyezési folyamatot.
Mivel minden felhasználó távoli, az engedélyezési folyamat azonos a hozzáférési jogosultságok igénylési engedélyezési eljárásával.

II.3.8. Mobil eszközök hozzáférés ellenőrzése

Az akkreditált informatikai rendszerhez korlátozás nélkül engedélyezett a mobil eszközökről történő hozzáférés. Amennyiben a későbbiekben a korlátozás lehetősége felmerül, akkor az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelős (IBF) bevonásával ki kell dolgozni annak technikai megvalósítását, a felhasználás feltételeit, korlátait és az engedélyezési folyamatot.
Ugyanakkor a mobil eszközök használatából származó kockázatokért az üzemeltető nem vonható felelősségre.

II.3.9. Külső akkreditált informatikai rendszerek használata

Az akkreditált informatikai rendszerhez jelenleg nem kapcsolódik semmilyen külső információs rendszer. Amennyiben a későbbiekben felmerül, hogy más rendszerek felé is kapcsolódnia kell az akkreditált informatikai rendszernek, akkor az üzemeltetőnek az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) bevonásával rögzíteni kell a két rendszer közötti szabványos interfész részleteit és a kapcsolódási pontokat.

II.3.10. Nyilvánosan elérhető tartalom

Az akkreditált informatikai rendszer közvetlenül nem tesz közzé nyilvánosan elérhető tartalmakat.
Amennyiben a későbbiekben ilyen felmerül, akkor erre vonatkozóan az informatikai rendszer üzemeltetőjének felelőssége kijelölni azokat a személyeket, akik jogosultak nyilvánosan elérhető tartalmak közzétételére. Az üzemeltetőnek a kijelölt személyeket oktatni kell annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető adatok ne tartalmazzanak nem nyilvános információt. A közzététel előtt az informatikai rendszert üzemeltető szervezet dokumentáltan átvizsgálja a közzétételre szánt anyagokat. Igény esetén kötelesek bevonni a folyamatba a Nemzeti Kommunikációs Hivatal kijelölt munkatársait.

II.4. Adathordozók védelme

Az akkreditált informatikai rendszer adatait saját tulajdonú adathordozókon kell tárolni. A felhőben történő adattárolás kifejezetten tilos. Az adathordozókat védeni kell az illetéktelen hozzáféréstől az alábbiakban leírtak szerint.

II.4.1. Adathordozók védelmére vonatkozó eljárásrend

Az akkreditált informatikai rendszer adathordozóihoz való hozzáféréseket, azok használatát, illetve törlését az üzemeltető vonatkozó eljárásrendjében foglaltak szerint kell kezelni. Mivel az akkreditált informatikai rendszer üzembe helyezése új adathordozók telepítésével jár, az üzemeltető feladata saját adathordozó nyilvántartásának kiegészítése.

II.4.2. Hozzáférés az adathordozókhoz

Az üzemeltető feladata kitölteni az alábbi táblázatot és az érintetteket tájékoztatni annak tartalmáról.
Az akkreditált informatikai rendszeren belül engedélyezett adathordozók:

Adathordozó típus	Szerepkör	Hozzáférés, jogosítvány
Akkreditált informatikai rendszer háttértárai	Rendszergazda	Fizikai, logikai – karbantartás, mentés
	A rendszer által kezelt üzleti folyamatokban részt vevő munkatárs	Logikai, szerepkörnek megfelelően
Mentés adathordozója	Rendszergazda	Fizikai, logikai – karbantartás, mentés, visszaállítás
	Adatgazda	Fizikai – mentések biztonságos tárolása
Rendszerelemek telepítő adathordozói	Rendszergazda	Fizikai, logikai – tárolás, telepítés
Vészhelyzeti adatokat (ÜFT, KET, vészhelyzeti működéshez szükséges adatok) tároló háttértárak	A vonatkozó szabályozásban megadott szereplők	A vészhelyzet kezelésével kapcsolatos, az ÜFT-ben és KET-ben leírt műveletek elvégzése és a vonatkozó dokumentumok karbantartása.

Az üzemeltető szervezet az adathordozók használatát információbiztonsági megfontolásból hardveres, illetve szoftveres úton korlátozhatja. A korlátozáshoz kapcsolódó kontrollok kidolgozása és bevezetése az üzemeltető felelőssége.

II.4.3. Adathordozók törlése

Az infokommunikációs eszközök újrahasznosítása vagy mások rendelkezésre bocsátása előtt minden esetben gondoskodni kell arról, hogy az akkreditált informatikai rendszerben használt adathordozókon tárolt információk visszaállíthatatlanul eltávolításra kerüljenek. Amennyiben a fejlesztési időszakban (a rendszer bevezetési projekt időtartama alatt) törölni kell egy adathordozót, az üzemeltető felelőssége a kapcsolódó szabályzatban leírtak szerint törölni az adathordozót.

Ennek érdekében:

- a rajtuk tárolt adatokat helyreállíthatatlanságot biztosító törlési technikákkal törölni kell; (biztonságos törlést biztosító eszközzel). HDD merevlemezek törlésénél olyan szoftvert kell alkalmazni, amely legalább 3x felülírja az adatot a törlés során, melyek közül legalább 1 felülírás véletlenszerű értékekkel történik. Amennyiben ez nem lehetséges (pl. SSD-k esetében), akkor az adathordozót kötelező elzárt helyen, dokumentáltan tárolni, és/vagy biztonságos és környezettudatos módon, dokumentáltan kell megsemmisíteni.
- a törlést az üzemeltető rendszergazdájának jóvá kell hagynia és felügyelnie kell;
- garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az üzemeltető Információbiztonsági Felelőse (IBF) dönt az eszköz cserére történő kiadhatóságáról.

Az adatok megfelelő módon történő eltávolításáért az üzemeltető felelős. Az adatok eltávolítását a rendszergazda végzi, vagy felügyeli. Az adat eltávolításának tényét és módszerét jegyzőkönyvezni kell.

II.4.4. Adathordozók használata

Az akkreditált informatikai rendszerrel kapcsolatban csak az üzemeltető tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszer bevezetési projekt során jelezni kell és a rendszergazdához kell benyújtani.

Az eszközhasználatot, a rendszerhez történő csatlakoztatása után az üzemeltető köteles minden előzetes értesítés nélkül figyelni, monitorozni.

Az akkreditált informatikai rendszerből adatot kinyerni (például tesztkörnyezetben munkavégzés céljából) csak az adatgazda írásos engedélyével lehetséges. Az adatok kivitelét írásos formában kell engedélyezni az adatgazdától, adathordozótól (optikai lemez, memóriakártya, elektronikus levél stb.) függetlenül.

II.5. Személyi biztonság

Az informatikai rendszert üzemeltető szervezet érintett munkavállalóinak kötelességei:

- Az informatikai rendszert, annak adatait az előírásoknak, kézikönyveknek, útmutatóknak megfelelően, rendeltetésszerűen használni, annak hibáit, biztonsági hiányosságait észleléskor jelenteni;
- A hitelesítő eszközeiket (jelszó, birtoklás alapú hitelesítő eszközök) saját ellenőrzés alatt tartani, azok megismerését, birtoklását harmadik fél számára lehetetlenné tenni. Ezek kompromittálódását haladéktalanul jelenteni;
- A szabályzatokban megfogalmazott internetes viselkedési szabályokat betartani;
- Az informatikai rendszer adatait maximális körültekintéssel kezelni, azok bizalmasságát és integritását megőrizni;
- Az informatikai rendszert üzemeltető szervezet szakmai vezetőjének, kapcsolattartójának a rendszerrel kapcsolatos utasításait követni;
- A szabályzatokat a rendszer kezelésének megkezdése előtt megismerni és erről nyilatkozatot tenni.

Az érintettek által aláírt nyilatkozatot az üzemeltető kötelessége megőrizni és igény esetén bemutatni a Nemzeti Kommunikációs Hivatal képviselőjének.

III. Visszamenőleg is nyomon követendő rendszerparaméterek

Az első alfejezet az MK rendeletben megjelölt, visszamenőleg is nyomon követendő rendszerparaméterekkel kapcsolatos, tételesen meghatározott követelmények részletezését tartalmazza. A további alfejezetek a követelményekhez kapcsolódó részletesebb biztonsági és funkcionális elvárásokat írják le.

III.1. A jogszabályi elvárásokkal kapcsolatos követelmények

Az alábbiakban az MK rendeletben tételesen megfogalmazott elvárások és követelmények pontosítását adjuk meg a rendeletben szereplő szerkezetnek megfelelően. Az egyes későbbi fejezetek az alábbi elvárásokat tovább részletezhetik még.

Az MK rendelet 7. § értelmében a nyomon követendő rendszerparaméterek:

a) a bejelentkezett felhasználók számának időbeli változása szerepkör és jogosultsági szint szerint:

Az informatikai rendszerben az adatok tárolásának végégig visszamenőleg elérhetőnek kell lennie az összes regisztrált felhasználó adatának. Kérésre bármelyik időpontról meg kell tudnia mondania a rendszer üzemeltetőjének, hogy milyen felhasználók (név, szerepkör, jogosultság, státusz) voltak a rendszerben.

b) a beszerzési eljárások állapota:

Elvárás, hogy az informatikai rendszerből kinyerhető legyen minden korábbi időpontról minden beszerzési eljárás állapota. Minimálisan az alábbi adattartalomnak visszakereshetőnek kell lennie:

- a beszerzésben érintett felek
- a beszerzés során megvalósításra kerülő egyes tevékenységek aktuális státusza
- a beszerzés adatai

c) az informatikai rendszer terheltsége:

Elvárás, hogy az informatikai rendszer minden korábbi időpontjáról – napi átlag értékeket tekintve – megállapítható legyen a rendszer terheltsége (memória foglaltság, diszk kapacitás, processzor terheltség). A követelmény teljesítésének célja, hogy az üzemeltető képes legyen biztosítani a folyamatos magas rendelkezésre állást.

d) átlagos válaszidők:

Elvárás, hogy az informatikai rendszer minden korábbi időpontjáról megállapítható legyen a rendszer aktuális válaszideje.

III.2. Naplózás és elszámoltathatóság

III.2.1. Naplózási eljárásrend

A naplózás és elszámoltathatóság megvalósulásának érdekében az alábbi eljárásrendet kell alkalmaznia az üzemeltetőnek. Szükség esetén a NIST 800-92-es ajánlása alapján az üzemeltető javaslatot tehet jelen eljárásrend módosítására.

III.2.2. Naplózandó események

Az üzemeltető kötelessége, hogy az akkreditált informatikai rendszer biztosítsa a következő események naplózását:

- Minden felhasználó vonatkozásában a felhasználók autentikációs tevékenysége:
    - bejelentkezés,
    - kijelentkezés,
    - jelszómódosítás;
- Az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;
- A rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;

- A rendszergazdák tevékenysége a rendszer bármely rétegében;
- A felhasználói jogosultságok módosítása;
- Rendszer események, esetleges hibák;
- Konfigurációs beállítások módosítása.

Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóban kell rögzíteni.
A rendszer naplózásának kialakításakor be kell vonni az informatikai rendszert üzemeltető szervezet részéről kijelölt rendszer-adatgazdát is annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletismeretek, amelyek a felhasználói tevékenységek nyomon követéséhez szükségesek.
A naplózási beállításokat az informatikai rendszert üzemeltető szervezet, valamint az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) az akkreditált informatikai rendszer bevezetése során bármikor felülvizsgálhatja annak érdekében, hogy elengedőek-e a biztonsági események kivizsgálásához. Az üzemeltető kötelessége beépíteni minden változtatásra irányuló kérést.

III.2.3. Naplóbejegyzések tartalma

Az akkreditált informatikai rendszerben a naplóbejegyzéseknek a következőket kell tartalmaznia:

- A rendszerelem azonosítóját;
- Az adatazonosítót (fájl / rekord / mező);
- Az esemény ismertetését / a funkcióazonosítót;
- A felhasználó azonosítóját;
- Az esemény időpontját;
- Az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

A naplóbejegyzések tartalmi megfelelőségéért az üzemeltető felel.

III.2.4. Napló tárkapacitás

A naplók tárkapacitását az üzemeltető kötelessége megtervezni, tudva azt, hogy naptári évenként legalább tízezer beszerzési eljárás adatainak tárolására és folyamatainak kezelésére alkalmas rendszerről van szó, illetve a naplók megőrzési ideje egy év. Üzemeltető kötelessége továbbá a kapacitástervezési folyamat kialakítása, amellyel a későbbiekben a rendszergazda a kapacitásigényt önállóan is tervezni képes.
A napló tárkapacitás figyelését a rendszerek felügyeleti tevékenységébe kell beépítenie az üzemeltetőnek.
A naplózást úgy kell beállítani, hogy amennyiben a naplóállomány eléri a kritikus mennyiséget, úgy automatikusan kerüljön archiválásra a napló, ezzel biztosítva a naplóbejegyzések felülírásának megakadályozását. Ezen túlmenően szükséges, hogy a rendszer automatikus értesítést küldjön a rendszergazdának, amennyiben a tárkapacitás növeléséről kell gondoskodni.

III.2.5. Naplózási hiba kezelése

Az akkreditált informatikai rendszerben a naplók figyelését oly módon kell kialakítani, hogy naplózási hiba esetén küldjön riasztást a rendszert üzemeltető rendszergazdáknak. Az üzemeltető feladata gondoskodni arról, hogy a rendszergazdák megfelelő oktatásban részesüljenek arról, mi a teendőjük az egyes riasztástípusok esetében.

III.2.6. Naplóvizsgálat és jelentéskészítés

Az akkreditált informatikai rendszerében az eseménynaplókat és biztonsági naplókat a napi üzemeltetési feladatok során át kell vizsgálni. Az üzemeltető feladata dokumentáltan rendelkezésre bocsátani a naplóvizsgálati eljárásrendet, valamint a rendszergazdákat megfelelő oktatásban részesíteni annak érdekében, hogy önállóan is képesek legyenek elvégezni a feladatot.
A hibabejegyzéseket és a szokatlan működésre utaló jeleket a Hibajavítás pontban leírtak alapján kell kezelni.

III.2.7. Időbélyegek

Az akkreditált informatikai rendszerben valamennyi naplóbejegyzést időbélyeggel kell ellátni, melyhez a rendszerórát kell alapul venni. A naplókban található időbélyegek helyi/UTC időket tartalmaznak.
Az üzemeltetőnek az akkreditált informatikai rendszert úgy kell kialakítani, hogy hálózati időszinkron protokoll segítségével szinkronizálja a rendszerórákat az egyezményes koordinált világidőhöz. Az üzemeltető hálózatában egy gépet kell szinkronizálni valamilyen külső forráshoz (pl. time.kfki.hu), az informatikai rendszert üzemeltető szervezet további belső elemei ehhez az eszközhöz szinkronizálnak (fa topológia szerint).
A Nemzeti Kommunikációs Hivatal által még tolerálható időeltérés 1 tizedmásodperc. Az üzemeltető feladata, hogy olyan rendszer kiépítéséről gondoskodjék, amelyben nincs két olyan elem, melyek között 1 tizedmásodpercnél nagyobb időeltérés alakulhat ki.

III.2.8. A naplóinformációk védelme

Az akkreditált informatikai rendszert az üzemeltető által kidolgozott eljárásrendben foglalt logikai védelmi intézkedések felhasználásával úgy kell kialakítani, hogy a naplóinformációk védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

III.2.9. A naplóbejegyzések megőrzése

A naplóinformációk mentését be kell vonni az akkreditált informatikai rendszer mentési rendszerébe. A mentési folyamat kialakítása és integrálása az üzemeltető felelőssége. A mentéseket a napló tárkapacitással összhangban úgy kell kialakítani, hogy a naplóbejegyzések nem veszhetnek el.
Az utólagos visszakereshetőség érdekében az akkreditált informatikai rendszer biztonsági naplóit 1 (egy) évig, míg a közbeszerzési folyamatok végrehajtásával és ellenőrzésével kapcsolatos naplókat 8 (nyolc) évig kell megőrizni.

III.2.10. Naplógenerálás

Az akkreditált informatikai rendszert fel kell készíteni a következő naplózással kapcsolatos követelmények teljesítésére:

- Biztosítania kell a naplóbejegyzések előállítási lehetőségét a Naplóbejegyzések tartalma pontban meghatározott naplózható eseményekre;
- Lehetővé kell tennie az üzemeltetésért felelős rendszergazdának és szükség szerint az Információbiztonsági Felelősnek (IBF) is annak kiválasztását, hogy mely naplózható események legyenek naplózva az akkreditált informatikai rendszer egyes elemeire;
- Naplóbejegyzéseket kell előállítania a Naplózandó események pontban meghatározottak szerinti eseményekre a naplóbejegyzések tartalma pontban meghatározott tartalommal.

A naplógeneráló rendszer üzemben tartása az üzemeltető kötelezettsége.

III.3. Biztonsági események kezelése

III.3.1. Folyamatos ellenőrzés

Az akkreditált informatikai rendszer belső kontrollrendszerében előírtak alapján, valamint az informatikai rendszert üzemeltető szervezet, vagy a Nemzeti Kommunikációs Hivatal ellenőrzési terve alapján folyamatosan ellenőrzi és ellenőrizheti az akkreditált informatikai rendszerek, rendszerelemek és szolgáltatások beszerzését és fejlesztését.
Az ellenőrzés során az alábbi kijelölt területekre fókuszálnak:

- a funkciók és kommunikációs csatornák megléte, illetve hogy nincs-e nem dokumentált funkcionalitás és kommunikáció a rendszerben,
- üzemeltetői változáskövetés, a rendszer csak a szükségszerű módosításokon esett át dokumentált módon, akár visszaállíthatóan,

- üzemeltető biztonsági tesztelés, mely tesztelési terv alapján kerül végrehajtásra dokumentált módon, igazolva a felfedezett hiányosságok javítását,
- üzemeltetői folyamat, melynek keretében a dokumentált, a szabályoknak és szabványoknak megfelelő üzemeltetési folyamat ellenőrzése történik,
- üzemeltetői oktatás, melynek keretében az akkreditált informatikai rendszer kiépítőitől a rendszer elemeinek oktatását várjuk el az informatikai rendszert üzemeltető szervezet munkatársai részére,
- az üzemeltetői biztonsági architektúra, mellyel kapcsolatosan elvárás, hogy illeszkedjen az informatikai rendszert üzemeltető szervezet biztonsági architektúrájához.

Az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) által az akkreditált informatikai rendszer ellenőrzését rendszeres és időszakos gyakorisággal dokumentált módon elvégzi. Az ellenőrzések eredményeit minden esetben értékelni kell biztonsági szempontból.

A Nemzeti Kommunikációs Hivatal a belső kontrollrendszerben előírtak alapján és/vagy ellenőrzési terv alapján elvégezheti:

- Az akkreditált informatikai rendszer biztonsági értékelését;
- A mérőszámok megfelelőségét;
- Az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;
- Az informatikai rendszert üzemeltető szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére.

Az üzemeltetőnek kötelessége eltűrni a Nemzeti Kommunikációs Hivatal illetékeseinek intézkedéseit.

III.3.2. Biztonsági eseménykezelési eljárás

Információbiztonsági eseménynek nevezzük a rendszer működésében beállt olyan kedvezőtlen változást, amelynek hatására a rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása, vagy a rendszer sértetlensége vagy rendelkezésre állása sérült vagy sérülhet.

A jellemző információbiztonsági események a következők:

- A szolgáltatás, a berendezés vagy az eszközök elvesztése;
- A rendszer hibás működése vagy túlterhelések (DoS-támadás);
- Emberi hibák;
- A szabályzatoknak vagy irányelveknek való nem megfelelés;
- A fizikai biztonsági rendelkezések megsértése;
- Nem ellenőrzött rendszerbeli változások;
- A szoftver vagy hardver hibás működése;
- Hozzáférési előírások megsértése;
- Kártékony kód általi fertőzés;
- A nem teljes vagy nem pontos működési adatokból eredő hibák;
- A bizalmasság és sértetlenség megsértése;
- A rendszerrel való visszaélés.

Az eseménykezelés során elsődleges cél a normál szolgáltatás lehető leggyorsabb helyreállítása és az üzleti folyamatokra gyakorolt káros hatás minimalizálása.

Az események kezelésekor a lehető leghamarabb mérséklő intézkedésnek kell születnie.

Az esemény tényét az akkreditált informatikai rendszerben alkalmazott űrlapon dokumentálni kell az eset későbbi kivizsgálása érdekében.

Az üzemeltető köteles követni az általa rögzített biztonsági eseménykezelési eljárását.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett információ-feldolgozó eszközt le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is. A meghibásodott eszközben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

A beérkezett jelentés alapján az Érintett szervezet Információbiztonsági Felelősének (IBF) feladata az esemény kivizsgálása és dokumentálása. Az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) kell javaslatot tennie a Nemzeti Kommunikációs Hivatal vezetője részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.
Az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) jelentenie kell az eseményt a jogszabályban meghatározott hatóságoknak.

III.3.3. A biztonsági események figyelése

A rendszer naplóinak, illetve a rendszer védelmét ellátó biztonsági eszközök naplóállományainak elemzésével, valamint a kialakított hibakezelési eljárások hatékony működtetésével az üzemeltető rendszergazdája és az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) folyamatosan figyelemmel kíséri a rendszerben bekövetkező információbiztonsági eseményeket.
Az üzemeltető felelőssége az újonnan bevezetett rendszerhez kapcsolódó új biztonsági események, és új monitoring lehetőségek megismertetése a rendszergazdával és az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősével (IBF).

III.3.4. A biztonsági események jelentése

Az észlelt biztonsági eseményeket azonnal jelenteni kell a rendszergazda és az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) részére. A hibaüzenetet (vagy az incidensre utaló jeleket) a felhasználó nem törölheti a képernyőről.
A felhasználó semmiféle kísérletet nem tehet a számítógép rendszert, vagy a hálózat működését érintő hiba megszüntetésére (még akkor sem, ha kellő felhasználói ismeretekkel rendelkezik), amíg az illetékes informatikai munkatárs azt nem látta (vagy a pontos hibaüzenetet, képernyőképet e-mailben el nem küldte a rendszergazda és az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) részére).
A rendszergazda, vagy az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) a hiba, incidens regisztrálása után köteles jelenteni a biztonsági eseményt a Nemzeti Kommunikációs Hivatal vezetőjének e-mailben és telefonon.

III.3.5. Segítségnyújtás a biztonsági események kezeléséhez

Az üzemeltető feladata, hogy tájékoztatást és segítséget nyújtson az akkreditált informatikai rendszer felhasználóinak az információbiztonsági események (incidensek) észlelése, kezelése és jelentése terén.

III.3.6. Biztonsági eseménykezelési terv

Az akkreditált informatikai rendszer kidolgozott információbiztonsági eseménykezelési tervvel rendelkezik, amely

- Iránymutatást ad az információbiztonsági események kezelési módjaira;
- Ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét;
- Átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe;
- Kielégíti az informatikai rendszert üzemeltető szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit;
- Meghatározza a bejelentés-köteles biztonsági eseményeket;
- Meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét;
- Támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére;
- Meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

Az üzemeltetőnek gondoskodnia kell arról, hogy

- A biztonsági eseménykezelési tervet ki kell hirdetni és tudomásul kell vetetni a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyekkel és szervezeti egységekkel;
- A biztonsági eseménykezelési tervet frissíteni kell és meghatározott gyakorisággal felül kell vizsgálni, figyelembe véve a rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;
- A biztonsági eseménykezelési terv változásait megismertesse az érintettekkel;
- A biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Az akkreditált informatikai rendszerben tapasztalt biztonsági események kezelését a tervnek megfelelően kell végrehajtani.

III.3.7. Képzés a biztonsági események kezelésére

Az információbiztonsági események (incidensek) megfelelő kezeléséhez és jelentéséhez szükséges ismeretek átadásáról az információbiztonsági oktatások keretében gondoskodni kell.

A rendszert üzemeltető rendszergazdákat, vezetőket, külső partnereket, felhasználókat, biztonsági felelősöket, adatgazdákat az információbiztonsági események kezelésével kapcsolatban történő képzésen a szerepkörüknek megfelelően kell informálni.

Az akkreditált informatikai rendszer vonatkozásában az információbiztonsági eseménykezelésről szóló képzésekre vonatkozó követelmények teljesítéséért az üzemeltető felel.

A biztonsági esemény kivizsgálásában csak olyan személynek vehetnek részt, akik megbízásuk előtt igazoltan részt vettek a biztonságiesemény-kezelő eljárásról szóló, a kormányzati eseménykezelő központ által tartott tájékoztató előadáson.

A felkészülésre kötelezettek jelenlegi köre:

- az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF)
- Rendszergazda

A felkészülésre kötelezettek körét az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) a későbbiekben bővítheti.

III.4. A rendszerek mentései

Rendszeresen biztonsági másolatokat kell készíteni az akkreditált informatikai rendszer által kezelt adatokról és a működését biztosító szoftverekről. Biztosítani kell a háttérkörnyezetet annak érdekében, hogy a lényeges adatok és szoftverek esetleges adathordozó hiba, a rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek.

Az akkreditált informatikai rendszer mentésének módját (szoftver, adathordozó, stb.) az üzemeltető joga megtervezni.

III.4.1. Üzleti adatok mentése

A rendszerben kezelt adatokról naponta 23 órakor teljes mentést kell készíteni. A napi mentéseken kívül heti és havi mentéseket is kell végezni. Napközben a naplózási rendszernek kellően részletes információt kell tárolnia az adatbázis tranzakciókról ahhoz, hogy a napi mentés és a napló segítségével visszaállítható legyen tetszőleges napközbeni állapot. A mentési megoldás kidolgozása és dokumentálása az üzemeltető feladata.

III.4.2. A rendszer mentése

Az akkreditált informatikai rendszer telepítésekor a rendszergazda technikai mentést végez a rendszerről, amit minden konfigurációváltoztatáskor és a változáskezelés hatálya alá eső, a rendszer működését befolyásoló beavatkozáskor ismételten elvégez. Az üzemeltető kötelessége segíteni a rendszergazdát feladata végrehajtásában.

III.4.3. Kapcsolódó dokumentációk mentése

A rendszergazda gondoskodik az akkreditált informatikai rendszerhez kapcsolódó dokumentációk, eljárásrendek, szabályzatok mentéséről és a mentés biztonságos helyen történő őrzéséről is. A dokumentáció elkészítése az üzemeltető feladata, és célszerűen segédkeznie kell a mentésben is.
A kapcsolódó dokumentációk mentését minden egyes változtatás esetén el kell végezni.

III.4.4. A mentések tárolása

Az akkreditált informatikai rendszer technikai mentéseit kettő példányban, biztonságos környezetben, páncélszekrényben kell őrizni. A mentéseket tilos a szerverekkel azonos területen (szerverteremben) tárolni. Az üzemeltető köteles a nála lévő üzleti adatokat tartalmazó mentéseket az akkreditált informatikai rendszer bevezetési projekt végével megsemmisíteni.

III.4.5. Adatok hosszú távú megőrzése

Az üzleti adatokat 15 (tizenöt) évig őrizni kell.
Ennek érdekében az üzleti adatok mentésére vonatkozóan a következő rotációs eljárásrendet (vagy ennél szigorúbbat) kell követni:

- Minden heti mentésből az utolsót havi mentésként meg kell őrizni.
- Minden havi mentésből az utolsót éves mentésként meg kell őrizni.
- Az éves mentéseket 15 (tizenöt) évig kell megőrizni.

Az üzemeltető követheti saját eljárásrendjét, vagy javasolhat másik eljárásrendet. Az üzemeltető kötelessége elfogadtatni a Nemzeti Kommunikációs Hivatal informatikai vezetőjével és elnökével saját rotációs eljárásrendjét az alkalmazott módszertannal egyetemben.

III.4.6. Mentési adathordozók kezelése

A mentésben aktívan részt vevő adathordozókat nyilvántartásba kell venni és visszakereshető formában kell tárolni. Az adathordozók cseréjére vonatkozó igényt az üzemeltető által meghatározott szoftver jelzi.

III.4.7. A helyreállítás tesztelése

A mentési eljárásrendeket úgy kell kialakítani, hogy az egyrészt megfeleljen az üzembiztonsági elvárásoknak, másrészt minél biztonságosabb védelmet nyújtson az esetlegesen előforduló hibák ellen.
Az alkalmazások fizikai védelme érdekében, gondoskodni kell arról, hogy a telepítő állományok ne károsodjanak, ezért az eredeti példányukról biztonsági másolatot kell készíteni és az eredeti példányokat át kell adni az akkreditált informatikai rendszer rendszergazdájának. Az üzemeltető csak a másolati példányokkal dolgozhat. Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tárolni. Az eredeti hordozókról készített másolatokat kell a napi tevékenység során használni. Az olvasási biztonság fenntartása érdekében az eredeti adathordozókról rendszeres időközönként frissítő mentést kell készíteni.

III.5. Biztonsági elemzés

III.5.1. Biztonságelemzési eljárásrend

Az üzemeltetőtől biztonsági értékelést kérünk a fejlesztett rendszer vonatkozásában. Az üzemeltető által végzett biztonsági elemzést a „NIST Special Publication 800-53A – Assessing Security and Privacy Controls in Federal Information Systems and Organisations” dokumentumban leírt módszertan alapján kell elvégezni.

III.5.2. Biztonsági értékelések

Az akkreditált informatikai rendszert üzemeltető szervezet biztonsági elemzés segítségével értékeli a kifejlesztett akkreditált informatikai rendszer és működési környezetének védelmi intézkedéseit. A biztonság elemzés célja az, hogy az informatikai rendszert üzemeltető szervezet meggyőződhessen róla, hogy a szükséges védelmi intézkedések megvalósítása megfelelően megtörtént, működésük a tervezettnek megfelelő.

Amennyiben a biztonsági elemzés eredménye alapján megállapíthatóak eltérések az akkreditált informatikai rendszer üzemeltetőjének biztonsági szabályzatai, eljárásrendjei és a gyakorlatban megvalósított megoldások között, az üzemeltető köteles azonnali intézkedéseket foganatosítani az eltérések megszüntetése érdekében.
A biztonsági elemzés az akkreditált informatikai rendszer üzemeltetőjének Informatikai Biztonsági Szabályzatában szereplő valamennyi adminisztratív, fizikai és logikai védelmi intézkedése vizsgálatára kiterjed.
A biztonsági elemzés által vizsgálandó valamennyi védelmi intézkedést az akkreditált informatikai rendszer bevezetési projekt során legalább kétszer (a tesztüzem elindítása előtt és az éles rendszer üzembe helyezése előtt) értékelni kell.
A biztonsági elemzés tervezéséért és végrehajtásáért az üzemeltető kijelölt munkatársai felelősek.
A biztonsági elemzés végrehajtásának támogatásához szükséges elkészíteni a biztonságelemzési tervet, amely a következőket tartalmazza:

- a vonatkozó védelmi intézkedések
- a biztonsági elemzés környezete
- a terv végrehajtásához szükséges személyi és technikai erőforrások
- a terv végrehajtása során alkalmazott technikák
- a terv végrehajtásához kapcsolódó szerepkörök és ezek feladatai
- a terv végrehajtásának üzemezése

A biztonságelemzési tervet végrehajtás előtt a vizsgált akkreditált informatikai rendszer adatgazdájának jóvá kell hagynia.
A biztonsági elemzés végrehajtásának eredményéről biztonságelemzési jelentés készül. A biztonságelemzési jelentés tartalmazza a következőket:

- az elvégzett tevékenység
- feltárt hiányosságok, sérülékenységek
- javasolt intézkedések és akciótervek

A biztonságelemzési jelentés kötelező jóváhagyója a vizsgált akkreditált informatikai rendszer adatgazdája.
A biztonságelemzési jelentés eredményeit az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF), és elnöke kapja meg, a kockázatelemzés folyamatában a későbbiekben felhasználja.

III.5.3. Az informatikai rendszer teljesítményének mérése

Az üzemeltetőnek feladata az akkreditált informatikai rendszereihez kifejleszteni az informatikai teljesítmény mérések rendszerét, melynek alapját a „NIST Special Publication 800-55 –Performance Measurement Guide for Information Security” dokumentumban található mérőszámok képezik.
A fejlesztett rendszer vonatkozásában minimálisan elvárt mérőszámokat az alábbi táblázat tartalmazza. Az üzemeltető további mérőszámokat határozhat meg a hivatkozott módszertan alapján.
Az üzemeltető által javasolt mérőszámokat és a kötelező mérőszámok kapcsán rögzítendő eljárásokat az üzemeltető kijelölt munkatársa egy külön dokumentumban hozza létre és hagyatja jóvá.
Az üzemeltető által kötelezően mérendő mérőszámok az alábbiak:

Mérőszám neve	Az akkreditált informatikai rendszer rendelkezésre-állása
Mérés célja	A mérés célja annak megállapítása, hogy a fejlesztett rendszer be tudja tölteni célját, rendelkezésre áll a feladat végrehajtására. Amennyiben nem elérhető a szolgáltatás, akkor a közbeszerzési folyamatok végrehajtási és ellenőrzési tevékenységek támogatása nyilván nem lehetséges.
Mérőszám meghatározása	A rendszer tökéletes működésre képes állapotú időtartama / Teljes idő (az osztó 168 óra)
Elérendő cél	Tesztüzemre: 99,0% Átadásra: 99,5%
Mérés gyakorisága	Hetente
Mérésért felelős	Üzemeltető által meghatározandó
Mérési adat forrása:	Felhasználói visszajelzések, valamint naplófájlok alapján az üzemeltető által javasolt (és

	jóváhagyott) metódus szerint

Mérőszám neve	Az akkreditált informatikai rendszer sebezhetőségeinek száma
Mérés célja	A mérés célja annak megállapítása, hogy a fejlesztett rendszer nem sérülékeny, ismert sebezhetőségeket nem tartalmaz
Mérőszám meghatározása	Az alkalmazott sebezhetőség-vizsgálati rendszer által szolgáltatott sebezhetőségi jelentésből a kritikus, magas kockázatú, közepes kockázatú és alacsony kockázatú sebezhetőségek számossága Az adatokat egy évre visszamenőleg is le lehessen kérdezni.
Elérendő cél	Kritikus sebezhetőségek száma: 0 a teljes időszakban Magas kockázatú sebezhetőségek száma: 0 a teljes időszakban Közepes kockázatú sebezhetőségek száma: 0, tesztüzemnél 1 még elfogadható Alacsony kockázatú sebezhetőségek száma: 1, tesztüzemnél 5 még elfogadható
Mérés gyakorisága	Mérföldkövenként
Mérésért felelős	Üzemeltető által meghatározandó, ám megfelelő minősítéssel (pl. CEH) rendelkező személy
Mérési adat forrása:	Az üzemeltető által javasolt (és jóváhagyott) eszköz segítségével előállított jegyzőkönyv

Mérőszám neve	A bejelentkezett felhasználók száma
Mérés célja	A mérés célja a rendszerbe bejelentkezett felhasználók számának követése szerepkör és jogosultsági szint szerint
Mérőszám meghatározása	A rendszerben lévő, bejelentkezett felhasználók száma az alábbi bontásban: • Nemzeti Kommunikációs Hivatal adminisztrátor fiókjai • Nemzeti Kommunikációs Hivatal engedélyező fiókjai • Nemzeti Kommunikációs Hivatal felhasználói fiókjai • Érintett szervezetek felhasználói fiókjai (összesen és a szervezetek szerint bontva) • Szállítók felhasználó fiókjai (összesen és a szállítók szerint bontva) Az adatokat egy évre visszamenőleg is le lehessen kérdezni.
Elérendő cél	Nem releváns
Mérés gyakorisága	Folyamatos, de legalább óránként egyszer.
Mérésért felelős	Az informatikai rendszer maga
Mérési adat forrása:	A rendszerben lévő autentikációs modul, illetve adatbázis

Mérőszám neve	Az informatikai rendszer terheltsége
Mérés célja	A mérés célja annak megállapítása, hogy az üzemeltetett rendszer nem került közel saját kapacitásának korlátaihoz.
Mérőszám meghatározása	Az informatikai rendszer mögött álló operációs rendszerek fizikai terheltsége, a processzorok, a memória és a háttértár vonatkozásában.
Elérendő cél	Processzorok terheltsége: az idő 95%-ában kevesebb, mint 50% Memória kihasználtság: az idő 95%-ában kevesebb, mint 50% Háttértár: az idő 95%-ában minimum 200GB szabad hellyel kell rendelkezni. Az adatokat egy évre visszamenőleg is le lehessen kérdezni.
Mérés gyakorisága	Folyamatos, de legalább percenként egyszer.
Mérésért felelős	Az informatikai rendszer maga.
Mérési adat forrása:	Az operációs rendszer(ek) által szolgáltatott információ. Virtualizált környezetben minden virtuális gép vonatkozásában külön-külön mérni kell.

Mérőszám neve	Az informatikai rendszer átlagos válaszideje.
Mérés célja	A mérés célja az informatikai rendszer átlagos válaszidejének (és ezáltal a használhatóságának) folyamatos nyomon követése.
Mérőszám meghatározása	A szerverrel egyazon alhálózatban lévő számítógépről indított szabványos HTTPS kérések és válaszok között eltelt idő: t1: A bejelentkező felület vonatkozásában a HTTPS-n elküldött GET kérés és a válasz utolsó bájtjának beérkezése között eltelt idő ms-ban. t2: A legbonyolultabb (legtöbb erőforrást igénylő, leghosszabb ideig tartó) adatbázis lekérdezéshez tartozó HTTPS kérés elküldése és a válasz utolsó bájtjának beérkezése között eltelt idő ms-ban. Az adatokat egy évre visszamenőleg is le lehessen kérdezni.
Elérendő cél	Az 1. pont vonatkozásában: t1 < 100 ms A 2. pont vonatkozásában: t2 < 1000 ms
Mérés gyakorisága	Folyamatos, de legalább óránként egyszer.
Mérésért felelős	Az informatikai rendszer maga
Mérési adat forrása:	A szerverrel megegyező alhálózatban lévő számítógép

Mérőszám neve	A beszerzési eljárások állapota
Mérés célja	A mérés célja a beszerzési eljárások állapotának folyamatos nyomon követése
Mérőszám meghatározása	Az adatbázisban lévő beszerzési eljárásokhoz kapcsolódó kumulált adatok. Az adatokat egy évre visszamenőleg is le lehessen kérdezni.
Elérendő cél	--
Mérés gyakorisága	Óránként.
Mérésért felelős	Az informatikai rendszer maga
Mérési adat forrása:	A beszerzési eljárások adatait tároló adatbázis(ok).

III.6. Konfigurációkezelés

Az üzemeltető konfigurációkezelési eljárásrendjének megfelelően a fejlesztett rendszer összetevőinek, konfigurációjának, telepített komponenseinek, változtatásainak, tesztjeinek és nyilvántartásának dokumentált módon rendelkezésre kell állnia.

III.6.1. Alap konfiguráció

Az implementált rendszerhez dokumentálni kell az alapkonfigurációt, amely a rendszer minden lényeges elemét (hardver és szoftver szinten) tartalmazza. Az alapkonfiguráció áttekintést ad a rendszerben tárolt szoftver és hardver elemekről, amelyet dokumentált formában, biztonságos körülmények között kell átadni a megbízó részére. Az alapkonfiguráció célja az, hogy alapjául szolgál egy esetleges jövőbeli rendszer újraépítéséhez. Ezért a rendszer minden fontos elemét, paraméterét dokumentált módon nyilván kell tartani.
A dokumentációnak minimálisan a következő elemeket kell magában foglalnia:

- Hardver elemek listája (szerver fizikai komponensei, esetleg hálózati eszközök, stb.);
- Szoftverek listáját aktuális verzió számmal, biztonsági frissítési információival és konfigurációs beállításaival, paramétereivel (operációs rendszer, alkalmazások, stb.);
- Telepítőkészletek listáját és elérhetőségi helyét (saját fejlesztés vonatkozásában);
- Egyes szoftverkomponensek alapkonfigurációit, beállításait (konkrét konfigurációs állományok és a kapcsolódó magyarázatok dokumentált formában);
- Hálózati topológia rajzot, amin követhető a rendszer komponensek logikai elhelyezkedése

Az akkreditált informatikai rendszer komponenseinek alapkonfigurációjára vonatkozó dokumentumot az üzemeltető készíti, szükség esetén (pl. a tesztüzem tapasztalatai alapján) felülvizsgálja, és a módosításokat átvezeti.

A fejlesztett rendszer valamennyi hardver/szoftver eleméről az üzemeltető rendszergazdájának nyilvántartást kell vezetni. Az üzemeltető kötelessége minden támogatást megadni ahhoz, hogy az üzemeltetőnél lévő nyilvántartás vetülete naprakész módon megtalálható legyen az üzemeltető saját belső nyilvántartásában.

III.6.2. A konfigurációváltozások felügyelete (változáskezelés)

Az üzemeltetőnél hatályban lévő változáskezelés szabályozásnak megfelelően szabad csak az akkreditált informatikai rendszert módosítani, vagy a konfigurációján változtatni. A biztonságos módosítás lehetőségei és folyamata az üzemeltető dokumentációjában elérhető. A naprakész rendszerállapot-információk elérhetőségének biztosítása az üzemeltető felelőssége.

Minden, az üzemeltetőnél futó rendszeren eszközölt változtatást megfelelően és visszakereshetően dokumentálni kell, amely alapján a változások egyértelműen megállapíthatóak és visszakereshetőek.

Minden egyes változást az üzemeltető megfelelően tesztel és dokumentál, mielőtt azt az éles rendszeren alkalmazná.

A fejlesztett rendszer esetében a következő tevékenységek tartoznak a változáskezelés hatálya alá:

- fejlesztések, verzióváltás,
- a rendszerelemek cseréje (legyen az hardver, vagy szoftver),
- a rendszerműködés, konfiguráció módosítása,
- a gyártó által kiadott frissítések telepítése.

Nem szükséges dokumentálni az üzemeltető saját (vagy idegen) fejlesztési környezetében eszközölt változtatásokat, ugyanakkor az éles és a tesztrendszer változásait is dokumentálni kell.

III.6.3. Változáskezelési előírások

A változáskezeléssel kapcsolatosan az alábbi előírásokat kell figyelembe venni az üzemeltetőnek:

- Az üzemeltetőnél futó rendszer bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is – az informatikai terület vezetőjének engedélye szükséges.
- Minden változtatással kapcsolatos bejelentés, véleményezés, döntés, a kivitelezés dokumentálása egy változáskezelési űrlap/kérelem és egy változáskezelési nyilvántartási táblázat kitöltésével jár együtt az Üzemeltető saját belső szabályzatának megfelelően.
- A változtatásokra vonatkozó valamennyi dokumentációt az üzemeltető informatikai területének nyilvántartásba kell venni és visszakereshető formában kell tárolnia, igény esetén be kell tudni mutatni.
- Az akkreditált informatikai rendszer bevezetési projektben nem szereplő változtatási igényt véleményezés céljából meg kell küldeni az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) is, aki kockázatelemzéssel megállapítja a tervezet változtatás rendszerre gyakorolt hatását.
- Az Információbiztonsági Felelősnek (IBF) a fentiek elvégzése után ellen kell jegyeznie a változtatási kérelmet.
- Az éles üzembe állítást csak a változással érintett adatok, rendszerek teljes mentését követően lehet elvégezni.
- Amennyiben a változtatáshoz a rendszer leállítása szükséges, akkor arról az informatikai terület a felhasználókat legalább 1 héttel megelőzően tájékoztatni köteles.

A változáskezelési előírásokat és a változáskezelési folyamatot az akkreditált informatikai rendszer biztonságáért felelős személy tartatja be az üzemeltetőnél.

III.6.4. Előzetes tesztelés és megerősítés

A változtatásokat (legyen az akár a tesztüzemből az éles üzemre való átállás) először tesztelni szükséges. A tesztkörnyezet nem tartalmazhat éles adatokat, illetve személyes adatokat. A tesztkörnyezetben a személyes

adatokat algoritmus felhasználásával anonimmá kell tenni. A tesztkörnyezetben lévő adatokért az üzemeltető felel.
A tesztkörnyezet jogosultsági beállításai, jogosultságkezelési folyamatai és adatbiztonsága az éles rendszerrel megegyező elvárásokat kell, hogy teljesítse. A teszt adatbázist teljes mértékben az eredetivel megegyező módon kell kezelni, a hozzáférés szabályozást is beleértve. A hozzáférés szabályozás klónozásáért az üzemeltető felel.
Az üzemeltetői teszteket az informatikai terület, a felhasználói teszteket a szakterület munkatársai, a biztonsági teszteket az Információbiztonsági Felelős (IBF) bevonásával kell elvégeznie az üzemeltetőnek.
A tesztelést dokumentált formában kell végezni, illetve a tesztek eredményeit dokumentálni kell, amely alapul szolgál a változtatás éles környezetben történő átvezethetőségére. A tesztelési dokumentáció elkészítéséért az üzemeltető a felelős.
Az éles rendszerben történő változtatás előtt frissíteni kell a rendszer valamennyi érintett dokumentációját, úgy, hogy az konzisztens legyen a véghezvitt változtatásokkal. A dokumentáció frissítéséért az üzemeltető a felelős.

III.6.5. Biztonsági hatásvizsgálat

Az üzemeltetőnek el kell fogadnia, hogy változtatás megkezdése előtt az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) egy előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható kockázatainak minimalizálását. Így a változtatások nem feltétlen tudnak a javasolt formában érvényre jutni, módosítási kérések érkezhetnek az Információbiztonsági Felelőstől (IBF).

III.6.6. Konfigurációs beállítások

A fejlesztett rendszer működtetése során csak jóváhagyott hardver és szoftver elemek használhatók, melyek az akkreditált informatikai rendszer rendszerdokumentációjában szerepelnek. A rendszer minden egyes eleméhez a konfigurációs beállításokat a kapcsolódó dokumentációban rögzített módon kell beállítani. Minden egyes módosítást, amely a konfiguráció beállításokhoz köthetőek, megfelelően dokumentálni kell (lásd a Konfigurációváltozások felügyelete pontot).
A kötelező, jóváhagyott konfigurációs beállításokat az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) az akkreditált informatikai rendszer bevezetési projekt során bármikor, a rendszerdokumentációban foglaltak alapján ellenőrizheti.

III.6.7. Legszűkebb funkcionalitás

Az akkreditált informatikai rendszert „a szükséges minimum elve alapján” úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, melyek a rendszer biztonságos működéséhez feltétlenül szükségesek. A rendszerben lévő eszközök funkcionalitását minimalizálni kell és szét kell választani úgy, hogy minden eszköz lehetőség szerint egy funkciót lásson el. Az akkreditált informatikai rendszer külön rendszeren kell, hogy megvalósuljon.
Az üzemeltetőnek az engedélyezett szolgáltatások listáját a rendszer rendszerdokumentációjában kell rögzíteni. A dokumentumot az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) és vezetője is jóvá kell hagyja.
Minden, a vizsgált akkreditált informatikai rendszerelemhez tartozó eszközön (szerver, kliensek, hálózati eszközök, stb.) kizárólag az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) által engedélyezett szoftverek kerülhetnek telepítésre. Ezért az üzemeltetőnek a rendszerdokumentációban fel kell tüntetni a szükséges szoftverkomponenseket, és azokat jóvá kell hagyatni az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) és vezetője által.
A kötelező, jóváhagyott szolgáltatásokat, portokat és protokollokat az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) az akkreditált informatikai rendszer bevezetési projekt során a rendszerdokumentációban foglaltak alapján ellenőrzi, szükség esetén javaslatot tesz a módosításra.

III.6.8. Akkreditált informatikai rendszerelem leltár

Az üzemeltetőnek leltárt kell vezetnie a saját rendszerének valamennyi eleméről (szoftver, illetve hardver elemekről egyaránt.) A Nemzeti Kommunikációs Hivatal munkatársai bármikor kérhetik a naprakész rendszerelem leltárt.
A leltárban fel kell tüntetni valamennyi hardvert, szoftvert és a vonatkozó dokumentációkat.
A leltárt az informatikai terület vezeti. Az informatikai területnek gondoskodnia kell a leltár teljességéről és naprakészségéről.
A leltárból egyértelműen azonosítani kell tudni, hogy az üzemeltetett rendszer területén található eszköz a rendszerhez tartozik vagy sem.

III.6.9. A szoftverhasználat korlátozásai

Az akkreditált informatikai rendszer működtetése során kizárólag jogtiszta, a megfelelő licenccel rendelkező szoftvereket lehet használni. Az üzemeltető felelőssége gondoskodni arról, hogy az újonnan telepítendő szoftverek jogtiszták legyenek.
Az alkalmazott szoftverekről leltárt kell vezetni (lásd a Rendszerelem leltár pontot).
Szabad vagy nyílt forráskódú szoftverek használatbavételét az üzemeltető informatikai terület vezetője engedélyezi dokumentált módon. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell. Az üzemeltető felelőssége gondoskodni a szükséges engedélyek beszerzéséről, amennyiben szükségesek.
Az üzemeltető felelőssége megfelelően megvédeni a telepítőkészleteket, illetve aktiválási kódokat az illetéktelen hozzáféréstől, felhasználástól.
A fejlesztett rendszeren nem lehetnek állomány megosztások.

III.6.10. A felhasználó által telepített szoftverek

Az akkreditált informatikai rendszeren megfelelő szoftvertelepítési politikát kell követni, a felhasználók számára nem szabad engedélyezni a szoftvertelepítést. A legszűkebb funkcionalitás elvéhez hasonlóan a felhasználóknak a legszűkebb, a munkavégzésükhöz még épp elegendő jogosultságokkal kell rendelkezniük. Így például a felhasználói csoport tagjai nem léphetnek be az operációs rendszer parancssorába, nem futtathatnak programokat.
A felhasználóknak ne legyen engedélyezett a szoftverfrissítések és egyéb biztonsági csomagok telepítésének elvégzése. A szabályok betartatása az üzemeltető felelőssége.

III.7. Ticketing rendszer

Az akkreditált informatikai rendszer megfelelő működéséhez ticketing rendszer szükséges. A biztonsági események (incidensek), hibás működés jelentését lehetővé tevő rendszerkomponens az új felhasználók felvételét, jogosultságok kiosztását, vagy módosítását is lehetővé tudja tenni (lásd később a követelményeket).
Elvárás, hogy a ticketing rendszer legyen alkalmas a nem lezárt folyamatok követésére. Támogatnia kell a hibák, incidensek állapotának követését, a ticketing rendszerben kezdeményezett jogosultságok módosítása vonatkozásában a folyamat státuszának követhetőségét (kinek a jóváhagyására vár a folyamat).
A ticketing rendszernek lehetőséget kell biztosítania prompt információk lekérésére a felhasználókhoz köthető hozzáférési jogosultságokról.
A ticketing rendszernek lehetőséget kell adni arra, hogy a múltban történt események visszakereshetőek legyenek a részt vállaló szereplők és az időpontok feltüntetésével.

III.8. Statisztikai adatgyűjtés és státuszképernyő

Az informatikai rendszernek alkalmasnak kell lennie arra, hogy a saját aktuális állapotáról a rendszergazdák számára könnyen értelmezhető módon tájékoztatást adjon. A státuszképernyőnek információt kell adnia az akkreditált informatikai rendszer mérőszámai (pl. rendelkezésre állás) vonatkozásában. A státuszképernyő mellett lehetőséget kell adnia különböző lekérdezés indítására, amely a háttérben lévő adatbázis vonatkozásában ad lehetőséget összesített információ, vagy jelentések kinyerésére.

A lekérdezési képernyőnek összesített adatokat kell szolgáltatni (pl. adott szervezethez kapcsolódó meghatározott időintervallumra eső közbeszerzési eljárások teljes értéke), tételes listákat is visszaadni (pl. adott közbeszerzési eljáráshoz kapcsolódó meghatározott időintervallumra eső tevékenységek). A lekérdezésekhez kapcsolódó feltételeknek a szokványos Boole algebra kapcsolatokkal egymáshoz köthetőnek kell lennie (ÉS/VAGY/XOR/NXOR), illetve negálhatók (NOT). Szükséges, hogy a lekérdezéshez kapcsolódó feltételek száma ne legyen korlátos, és tetszőleges kombináció összerakható legyen a felületen (zárójelezhetőség biztosítása).

IV. Funkcionális követelmények

Az első alfejezet az MK rendeletben tételesen meghatározott funkcionális követelmények kibontását tartalmazza. A további alfejezetek pedig a követelményekhez kapcsolódó részletesebb biztonsági és funkcionális elvárásokat írják le.

IV.1. A jogszabályi elvárásokkal kapcsolatos követelmények

Az alábbiakban az MK rendeletben tételesen megfogalmazott elvárások és követelmények pontosítását adjuk meg a rendeletben szereplő szerkezetnek megfelelően. Az egyes későbbi fejezetek az alábbi elvárásokat tovább részletezhetik még.

Az MK rendelet 8. § értelmében az informatikai rendszernek alkalmasnak kell lennie
a) a beszerzések teljesülésével kapcsolatos adatok valós idejű nyomon követése érdekében a tervek, megrendelések, vásárlási adatok, teljesítési igazolások és számlák feltöltésére:
Az akkreditált informatikai rendszernek alkalmasnak kell lennie a Beszerzések végrehajtásával, ellenőrzésével kapcsolatos adatok napi feltöltésére, bevitelére. Az adatok feltöltését megoldható mind kézi adatbevitellel, mind pedig dokumentumok csatolásával is. Amennyiben a rendszer támogatja a dokumentumok csatolását, akkor kezelnie kell az alábbi dokumentum típusokat: tervek, megrendelések, vásárlási adatok, teljesítési igazolások és számlák. A feltölthető dokumentumok esetében a rendszernek támogatnia kell az alábbi formátumokat: Microsoft Office (Word, Excel, Powerpoint), Open Document formátum, Adobe Pdf, kép állományok (Jpg, Tiff, Png, Bmp), szöveges állományok.

A rendszernek a Beszerzésekkel kapcsolatosan az alábbi adatokat kell tudnia kezelni:

- Beszerzések eredményeként kötött Szerződések
- Beszerzések eredményeként kötött szerződések Megrendelései
- Beszerzések eredményeként kötött szerződések Teljesítésigazolásai
- Beszerzések eredményeként kötött szerződések Számlái
- Szerződés törzsadatok
    - Érintett szervezet hivatkozás
    - Szállító hivatkozás
    - Termék/szolgáltatás kategória
    - Teljes nettó összeg
    - Kezdő dátum
- Termék/szolgáltatás kategória
    - Megnevezés
    - Mennyiségi egység (pl. darab, óra, egyéb)
    - Egységár/kedvezmény mérték

Szállító

- A Szállító a Beszerzés tervét elkészíti és a terv engedélyeztetését igényli.
- A teljesítést követően a Teljesítésigazolást engedélyezésre az Érintett szervezet számára továbbítja
- A Teljesítésigazolás alapján kiállított Számlákat az informatikai rendszerben rögzíti.

Érintett szervezet

- Az Érintett szervezet a Szállító által rögzített tervet engedélyezi.
- Az Érintett szervezet a beszerzés végrehajtása során előállt Teljesítésigazolásokat jóváhagyja.

b) az informatikai rendszerből származtatható adatokból, információkból nyert kimutatások készítésére:
Az informatikai rendszernek az alábbi kimutatásokat kell tudnia biztosítani a Nemzeti Kommunikációs Hivatal felhasználói számára:

- Beszerzések listája Szállítónkénti bontásban
- Beszerzések listája Érintett szervezetenkénti bontásban
- Beszerzések listája státuszok szerinti bontásban

A kimutatásoknak az egyes beszerzésekről tartalmazniuk kell az alábbiakat:

- Beszerzés státusza
- Beszerzésben érintett szereplők
- Beszerzés megnevezése
- Beszerzéssel kapcsolatos dátumok
- Beszerzés összege

c) dokumentált interfész kapcsolat biztosítására más állami közbeszerzési informatikai rendszerhez:

Az informatikai rendszernek tudnia kell kapcsolódni a Hivatal kormányzati kommunikációs beszerzések központi közbeszerzési informatikai rendszerével (a továbbiakban Portál) és az informatikai rendszer által szolgáltatott interfészen keresztül adatokat szinkronizálni a Portálon rendelkezésre álló adatok tekintetében. Az informatikai rendszer folyamatainak illeszkednie kell a Portálon belül megvalósított Beszerzés folyamataihoz és adataihoz.

A rendszer által megvalósított kapcsolódási lehetőség interfészét olyan szinten kell dokumentálni és a Nemzeti Kommunikációs Hivatal számára átadni, amely alapján egy külső fejlesztő a kapcsolódáshoz szükséges fejlesztéseket el tudja végezni.

IV.2. Általános védelmi intézkedések

IV.2.1. Az akkreditált informatikai rendszer kapcsolódásai

Az informatikai rendszert üzemeltető szervezet csak a felügyelete alatt álló akkreditált informatikai rendszer felett gyakorol kontrollt, a rendszer felügyelet nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett. Az informatikai rendszert üzemeltető szervezet munkavállalóinak felügyelete alatt álló, ideiglenes kapcsolatok – pl. adatok manuális letöltése más szervezetek informatikai rendszeréből – nem tartoznak e tiltás hatálya alá. Más szervezetek (pl. más állami) informatikai rendszerei (pl. közbeszerzési informatikai rendszerek) irányába az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) jóváhagyásával létesülhet kapcsolat.

Az akkreditált informatikai rendszerének összekapcsolását más szervezetek informatikai rendszerével csak előzetes hatásvizsgálat után engedélyezi az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF). Az engedélyezés feltétele, hogy a másik rendszer biztonsági szintje nem alacsonyabb a besorolásnál meghatározott szintnél (jelenleg adminisztratív biztonsági szint: 2, fizikai biztonsági szint: 2, logikai biztonsági szint: 3-3-3). Az összekapcsolást az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF-nek) jóvá kell hagynia. Az összekapcsolás feltételeinek fennálltát legalább évente ellenőrizni kell. Az engedélynek tartalmaznia kell az összeköttetés pontos paramétereit (cél, technikai megvalósítás, átvitt információk, biztonsági követelmények).

Számítógép hálózati kapcsolódás csak biztonságos kapcsolattal (TLS/SSL) lehetséges, amelynek elfogadható paramétereit a kriptográfiai fejezetben részletesen leírjuk.

IV.2.2. Belső rendszer kapcsolatok

Az akkreditált informatikai rendszert jelenleg nem kell semmilyen belső rendszerrel összekapcsolni.

A szervezet akkreditált informatikai rendszere és más (pl. fent felsorolt) komponensek között minden új kapcsolat kialakítása előtt a kapcsolat létrehozását az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének jóvá kell hagynia.

IV.2.3. Külső kapcsolódásokra vonatkozó korlátozások

Az akkreditált informatikai rendszer külső kapcsolatai vonatkozásában minden tiltott, ami nem megengedett (fehér lista elven alapul). Ennek megfelelően az akkreditált informatikai rendszer implementációja csak a HTTPS portot tarthatja nyitva. Minden külső kapcsolódási igényt előzetesen jelezni kell, hogy a szükséges beállítások időben rendelkezésre álljanak.
Az engedélyezési listát az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) hagyja jóvá és hirdeti ki.

IV.2.4. Személybiztonság

Az akkreditált informatikai rendszert implementáló és üzemeltető cég alkalmazottainak meg kell felelniük a Nemzeti Kommunikációs Hivatal alábbi elvárásainak: büntetlen előélet, legalább középfokú végzettség, alapszintű számítógépes ismeretek.

IV.3. Külső informatikai rendszerek szolgáltatásai

Az akkreditált informatikai rendszer üzemeltetője a külső szolgáltatótól szolgáltatási szerződés alapján igénybe vett, az akkreditált informatikai rendszer részét képező szolgáltatások esetén meg kell, hogy követelje, hogy az igénybe vett informatikai alrendszer, komponens, vagy szolgáltatás fizikai, logikai és adminisztratív vonatkozásaiban feleljenek meg az akkreditált informatikai rendszer üzemeltetője által előírt biztonsági követelményeknek.
Az üzemeltető meghatározza a felhasználók feladatait és kötelezettségeit az akkreditált informatikai rendszer külső szolgáltatásainak biztonságos használatával kapcsolatosan. A felhasználók az akkreditált informatikai rendszer külső szolgáltatótól igénybe vett részeit csak a szerződésben meghatározott hitelesítést követően ugyancsak a szerződésben meghatározott szintig vehetik igénybe. Az akkreditált informatikai rendszer külső szolgáltatótól igénybe vett szolgáltatás-biztonsági előírásai a belső elemekkel megegyezők, abban ismeretlen eredetű fájlok feldolgozása, ismeretlen folyamatok indítása tilos. A rendszer külső elemeinek működése során tapasztalt bármilyen rendellenességet, az elvárttól értérő működést azonnal jelenteni kell az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF).
A Nemzeti Kommunikációs Hivatal és az informatikai rendszert üzemeltető szervezet a rendelkezésére álló eszközökkel ellenőrizheti, hogy a szolgáltató biztosítja-e az elvárt biztonsági szintet és védelmi intézkedéseket. Az ellenőrzés történhet saját belső eszközökkel, illetve külső, harmadik fél szolgáltatásainak igénybe vételével.
Amennyiben a fejlesztő által készített rendszer szolgáltatásaihoz külső akkreditált informatikai rendszerbeli szolgáltatásokra van szükség, az informatikai rendszert üzemeltető feladata és felelőssége, hogy a partner teljesítse a Nemzeti Kommunikációs Hivatal által megfogalmazott követelményeket.

IV.4. Tesztelés, képzés és felügyelet

IV.4.1. Tesztelési, képzési és felügyeleti eljárások

Az üzemeltető feladata az elkészült rendszerre vonatkozóan egy teljes dokumentációs csokrot átadni, amelyben megtalálhatóak:

- fejlesztői dokumentáció, a későbbi továbbfejlesztések támogatása érdekében
- adminisztrátori dokumentáció, a rendszer üzemben tartásához, felügyeletéhez szükséges leírásokkal
- felhasználói dokumentáció, amely a rendszer használatát segíti.

A dokumentáción túl a Nemzeti Kommunikációs Hivatallal, az Érintett szervezetekkel, valamint a Szállítókkal egyeztetett időpontokban oktatást kell tartani a kijelölt kollégák számára. A felhasználói dokumentációhoz kapcsolódó oktatási anyagot át kell adni a Nemzeti Kommunikációs Hivatalnak, az érintett Szervezeteknek, valamint a Szállítóknak a további oktatások támogatása céljából.

IV.4.2. Sérülékenység teszt

Az üzemeltető köteles a szoftvert kereskedelmi forgalomban kapható (pl. Nessus) sebezhetőség-vizsgálati eszközzel tesztelni, a feltárt sebezhetőségeket megszüntetni az átadás előtt. A sebezhetőség vizsgálat elvégzését egy jegyzőkönyvvel kell igazolni, amelyhez a használt szoftver kimenetét is csatolni kell. A vizsgálatot csak megfelelő minősítéssel (pl. CEH) rendelkező személy végezheti.

Az üzemeltető feladata továbbá olyan munkautasítást létrehozni, amellyel az informatikai rendszert üzemeltető szervezet rendszergazdája évente meg tudja ismételni a szükséges vizsgálatokat. A rendszergazdának képessé kell válnia:

- A sérülékenységi tesztek futtatására
- Az elvégzett vizsgálatról jelentés készítésére, amelyben a hibák, nem megfelelően konfigurált elemek kerülnek kimutatásra
- hibaelhárítási javaslatok megfogalmazására, amellyel a hibák kijavíthatóak.

A sérülékenységi vizsgálatok koordinálásáért és kiértékeléséért az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) lesz felelős a későbbiekben (az átadás után).

IV.4.3. Frissítési képesség

A fejlesztés csak olyan eszközzel végezhető, amely megfelel az iparági sztenderdeknek, így képes a szoftverkomponenseit, szignatúráit nyilvánosan hozzáférhető központi adatbázisból, vagy a fejlesztő által az üzemeltető számára hozzáférhetővé tett forrásból frissíteni.

IV.4.4. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően

A fejlesztett rendszeren használt sérülékenység-vizsgáló szoftver szignatúra adatbázisát új vizsgálat megkezdése előtt frissíteni szükséges, így biztosítva, hogy a szoftver képes legyen a legutóbb megismert sérülékenységek felismerésére az akkreditált informatikai rendszerben.

Amennyiben a vizsgálat valamilyen sérülékenységet azonosított és az szoftverkomponensek frissítésével orvosolható, az üzemeltető köteles azonnali hatállyal gondoskodni a frissítés végrehajtásáról. Egyéb esetben cselekvési terv készül (lásd a cselekvési terv pontban) a rendszer bevezetési projekt-terv kiegészítéseként, amelyben az üzemeltető meghatározza a szükséges módosítások és konfigurációs változtatások menetrendjét.

IV.4.5. Privilegizált hozzáférés

Az akkreditált informatikai rendszerhez az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelős (IBF) által ellenőrzött és dokumentált körülmények közt az üzemeltető privilegizált hozzáférést is biztosít a sérülékenységi vizsgálatot végző személy(ek)nek a vizsgálat idejére.

IV.4.6. Felfedhető információk

A sérülékenységi vizsgálat után az üzemeltetőnek értékelési dokumentációban fel kell mérnie, hogy egy támadó milyen érzékeny adatokhoz lehet képes hozzáférni az akkreditált informatikai rendszer információvagyonából.

A vizsgálat eredményéről készült dokumentumot az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF) is át kell adni a sérülékenység vizsgálat után a lehető leghamarabb, de legkésőbb öt munkanapon belül.

IV.5. Karbantartás

IV.5.1. Rendszer karbantartási eljárásrend

A folyamatos működés érdekében az akkreditált informatikai rendszert rendszeresen karban kell tartania az üzemeltetőnek. A karbantartási tevékenységnek ki kell terjednie a hardver és szoftver eszközök karbantartására egyaránt. Az üzemeltető karbantartásra vonatkozó követelményeit, ajánlásait és eljárásrendjét dokumentálni szükséges. A dokumentum elkészítése az üzemeltető felelőssége. A karbantartási eljárásrendben szerepeltetni kell a karbantartási feladatok ütemezését is (pl. évente, 3 havonta, stb.).

IV.5.2. Rendszeres karbantartás

A folyamatos működés érdekében az akkreditált informatikai rendszert rendszeresen karban kell tartani. A rendszer bevezetési projektje során is szükségessé válhat karbantartási feladat. Ebben a pontban a karbantartási tevékenységgel kapcsolatos, általános szabályokról esik szó. Amennyiben karbantartási feladat adódna, az üzemeltető felelőssége az itt leírtak alapján eljárni.

IV.5.3. A karbantartások engedélyezése

A tervezett karbantartásokat az üzemeltető informatikai terület vezetőjének dokumentált formában kell engedélyeznie. Amennyiben a karbantartás az akkreditált informatikai rendszer leállításával jár, akkor a felhasználókat a karbantartás megkezdése előtt legalább egy héttel értesíteni szükséges. Az engedélyek beszerzése és az értesítés foganatosítása az üzemeltető felelőssége.

IV.5.4. A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét az üzemeltetőnél található karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani. A karbantartásról jegyzőkönyv készül, amelyben a következő adatokat kell minimálisan rögzíteni:

- az elvégzett karbantartási tevékenység megnevezése;
- az érintett hardver/szoftver eszközök, akkreditált informatikai rendszer elemek azonosítása;
- cserélt alkatrészek pontos megnevezése (új alkatrész, régi alkatrész gyári száma)
- a karbantartás engedélyezője;
- a karbantartás elvégzője;
- a karbantartást felügyelő személy;
- a karbantartás dátuma, hossza (időben);
- leállási idő (ha volt ilyen);
- a biztonsági ellenőrzés végrehatása;

A jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz. A karbantartással kapcsolatos dokumentumokat bármikor kérhetik a Nemzeti Kommunikációs Hivatal erre feljogosított munkatársai.

IV.5.5. A karbantartások ütemezése

Az üzemeltető által készített, az akkreditált informatikai rendszerre vonatkozó karbantartási eljárásrendnek része a karbantartások ütemezése (lásd a Rendszerkarbantartás pontot). Az éves karbantartási terv elkészítése az üzemeltető informatikai vezetőjének feladata, a terv jóváhagyása a Hivatal vezetőjének feladata.

IV.5.6. Kiszállítás

Amennyiben a karbantartási tevékenység során adatot tartalmazó adathordozó kiszállítása válik szükségessé, az elszállítás előtt az üzemeltető rendszergazdája minden adatot és információt – mentést követően – töröl a berendezésről. Mivel a rendszergazda nem ismerheti a fejlesztés alatt lévő rendszer minden komponensét, az üzemeltető felelőssége figyelmeztetni a rendszergazdát, ha van adathordozó a kiszállított berendezésben. A törlés a rendszergazda felelőssége.

Informatikai eszköz csak engedély birtokában legyen kiszállítható. A kiszállítást az informatikai terület vezetője (vagy felettese) engedélyezheti.

IV.5.7. A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikeres teszt esetén az eszköz ismételten éles üzembe helyezhető. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe. Az eseményt jelenteni kell az informatikai terület vezetőjének, aki dönt a további intézkedésekről.

IV.6. Rendszer és információ sértetlenség

Az akkreditált informatikai rendszer rendszer- és információsértetlenségre vonatkozó rendelkezéseit tartalmazó eljárásrend kidolgozása és jóváhagyatása az üzemeltető feladata. Az eljárásrendet a Nemzeti Kommunikációs Hivatal informatikai vezetője és elnöke hagyja jóvá.

IV.6.1. Rendszer és információ sértetlenségre vonatkozó eljárásrend

Az akkreditált informatikai rendszer, illetve az abban kezelt adatok sértetlenségének biztosítása érdekében az üzemeltető kötelessége a rendszerdokumentációban kitérni a rendszer- és információ sértetlenség biztosítását célzó eljárásrendre. Az eljárásrendben minimálisan az alábbi elemeknek kell szerepelni.

IV.6.2. Hibajavítás

Az akkreditált informatikai rendszerben keletkező hibákat az üzemeltető saját eljárásrendjének előírásai szerint, megfelelően kezeli.
A hibák javítását és kezelését a rendszergazdák végzik, illetve koordinálják.

IV.6.2.1. Szoftverfrissítések

A szoftverfrissítések telepítése változáskezelési eljárás hatálya alá tartozik, ezért ebben az esetben a Konfigurációváltozások felügyelete pontban leírtak alkalmazandóak, azzal a kiegészítéssel, hogy a telepítés előtt különös figyelmet kell fordítani a frissítés tesztkörnyezetben történő tesztelésére.

IV.6.2.2. Biztonsági frissítések

A rendszer biztonsági frissítéseinek telepítése szintén a változáskezelési eljárás hatálya alá tartozik, ezért ebben az esetben a Konfigurációváltozások felügyelete pontban leírtak alkalmazandóak a következőkkel kiegészítve:
A biztonsági frissítések éles környezetben történő telepítését meg kell előznie egy – az informatikai rendszert üzemeltető szervezet jellemző eszközeiből felépített reprezentatív – tesztkörnyezetben való tesztelésnek.
A tesztelést a biztonsági frissítés kiadását követő 1 héten belül el kell végezni. Törekedni kell arra, hogy a biztonsági frissítések a kiadást követő 3 héten belül telepítésre kerüljenek valamennyi érintett eszközre.

IV.6.2.3. Microsoft termékek biztonsági frissítéseinek telepítése

A Microsoft termékek biztonsági frissítéseinek telepítésére a Microsoft által biztosított központi menedzsment terméket kell alkalmazni, mely biztosítja a frissítések ütemezését, a munkaállomások és a kiszolgálók újraindításának kikényszerítését, a telepítési műveletek naplózását.

IV.6.2.4. Nem Microsoft termékek biztonsági frissítéseinek telepítése

A nem Microsoft termékek frissítését a gyártói ajánlások figyelembe vételével kell elvégezni.

IV.6.3. Kártékony kódok elleni védelem

Az üzemeltetőnek meg kell őriznie az akkreditált informatikai rendszer és az abban tárolt információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek támadásaival szemben.
Ezért az üzemeltetőnek a kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

- Kártékony kód elleni megoldás nélkül önálló munkaállomás nem üzemeltethető.
- A rendszeren úgy kell a kártékony kódirtó alkalmazást konfigurálni, hogy memóriában rezidensként fusson, valamint hetente egyszer ütemezett, teljes körű ellenőrzést futtasson le.
- A memóriában rezidens modul ellenőrzésének minden írási és olvasási műveletre ki kell terjednie.
- Folyamatok, könyvtárak és állományok kizárása a kártékony kód elleni védekezés alól csak a legkorlátozottabb módon, előzetes jóváhagyást követően, előzetesen tesztelt módon, az elektronikus rendszer dokumentációjában rögzített módon történhet.

- Kártékony kód általi fertőzés esetén elsődleges akcióként próbálja meg tisztítani, ha az sikertelen, akkor semmisítse meg a kártékony kódot.
- Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.
- A kártékony kód elleni alkalmazások adatbázisát rendszeresen, a szállító által meghatározott ütemezéssel, vagy automatikusan frissíteni kell.
- A kártékony kód elleni alkalmazáshoz tartozó szoftverfrissítések kezelése a változáskezelés és konfigurációkezelés hatálya alá esik.
- A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.
- A külső forrásból származó cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.
- A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.
- A kártékony kódirtó rendszert úgy kell konfigurálni, hogy riasztás esetén automatikusan elektronikus levélben értesítse az üzemeltető rendszergazdáit és az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősét (IBF).
- A kártékony kód észlelésével és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

Kártékony kód ellen minden rendszerkomponensen védekezni kell, legyen az tetszőleges operációs rendszerű. Pl. Linux, vagy BSD rendszerek alkalmazása esetében is szükséges védekezni a kártékony kódok ellen!

IV.6.4. Az akkreditált informatikai rendszer felügyelete

Az akkreditált informatikai rendszerének napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása. Az üzemeltetőnek ezért gondoskodnia kell az akkreditált informatikai rendszer vonatkozásában az alábbiakról:

A rendszer felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

A fenti feladatok végrehajtásának megszervezése és koordinálása az informatikai terület vezetőjének, a feladatok végrehajtása az érintett rendszergazdák feladata. A végrehajthatóság és megszervezhetőség biztosítása az üzemeltető felelőssége.

Ezért az üzemeltetőnek az eljárásokat üzemeltetési szabályzatban/eljárásrendben kell rögzíteni, melyet egyeztetni szükséges az informatikai terület vezetőjével. Az eljárásrendben az alábbiakat kell rögzíteni:

Valamennyi kritikus rendszer vonatkozásában ki kell jelölni az üzemeltetési felelősöket. A feladatokat és felelősségeket rögzíteni kell az érintett munkatárs munkaköri leírásában is.

A rendszergazdának ismernie kell az informatikai rendszert üzemeltető szervezet rendszereszközeinek, az akkreditált informatikai rendszereinek működését és azok figyelmeztető és hibaüzeneteit. A szükséges reagálásokat tartalmazó leírást az üzemeltetőnek kell elkészítenie és oktatnia. A rendszergazdáknak készség szinten kell tudniuk alkalmazni a leírásban foglaltakat.

A rendszergazdának rendszeresen el kell végeznie azokat a tevékenységeket, amelyek alapján meggyőződhet arról, hogy a rendszer üzemszerűen működik. A tevékenység leírását az üzemeltető kötelessége dokumentált formában rendelkezésre bocsátani.

Az üzemeltetési eljárások megfelelőségét az akkreditált informatikai rendszer bevezetési projekt során az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelőse (IBF) felülvizsgálhatja, illetve kérheti a módosítását. A szükséges módosítások átvezetése az üzemeltető feladata, az illetékes felelős vezető jóváhagyása mellett.

IV.6.5. Biztonsági riasztások és tájékoztatások

Az üzemeltető Információbiztonsági Felelősének (IBF) feladata a következő, jogszabályban kijelölt szervezetekkel történő kapcsolattartás:

- Nemzeti Elektronikus Információbiztonsági Hatóság
- Kormányzati Eseménykezelő Központ
- Nemzeti Biztonsági Felügyelet

A Szervezet a jogszabályban meghatározottak szerint bejelenti a Nemzeti Elektronikus Információbiztonsági Hatóság és a Kormányzati Eseménykezelő Központ részére az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelős (IBF) azonosító adatait, ezzel megteremti a kapcsolattartás feltételeit az információbiztonság felügyeletével megbízott kormányzati szervekkel.

Az Információbiztonsági Felelősnek (IBF) folyamatosan figyelemmel kell kísérnie a fenti szervezetek által kiadott riasztásokat és gondoskodnia kell a rendszerre vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről.

Amennyiben azonban az üzemeltető azt tapasztalja, hogy a riasztás érinti az akkreditált informatikai rendszerét, vagy felhasználóit, akkor az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősét (IBF) és az érintett felhasználókat elektronikus levélben értesíteni köteles a riasztásban foglaltakról. Az üzemeltető köteles továbbá segédkezni a védelmi intézkedések kidolgozásában és bevezetésében. Az üzemeltető felelőssége, hogy felhívja a felhasználók figyelmét a felhasználói oldalról követendő magatartásra a bevezetett rendszer kapcsán.

IV.6.6. A kimeneti információ kezelése és megőrzése

A kimeneti információ (pl.: nyomtatás, naplók, számlák, elektronikus adatok) kezelésével és szétosztásával kapcsolatban az akkreditált informatikai rendszert üzemeltető Iratkezelési Szabályzatával összhangban a következők az előírások:

- gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről;
- gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon;
- gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.

Az üzemeltetőnek biztosítania kell, hogy a fenti pontok teljesüljenek az akkreditált informatikai rendszer vonatkozásában is. Biztosítani kell továbbá, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

IV.7. Rendszer- és kommunikáció védelem

IV.7.1. Rendszer- és kommunikáció védelmi eljárásrend

Az akkreditált informatikai rendszer és a rendszer kommunikációjának védelme érdekében az üzemeltetőnek egy eljárásrendet kell kidolgozni és alkalmazni. Az eljárásrend megismertetése a rendszergazdákkal az üzemeltető kötelessége.

IV.7.2. Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem

Az akkreditált informatikai rendszert fel kell készíteni a szolgáltatás megtagadás (Denial of Service – DoS) alapú támadásokkal szemben.

Ennek érdekében biztosítani kell az érintett rendszert alkotó szoftverek naprakészségét a Hibajavítás pontban leírtak szerint.

Az érintett rendszer kártékony kód elleni védelmét a Kártékony kódok elleni védelem pontban leírtak szerint kell megvalósítani.

A határok védelmét a következő pontban leírtak alapján kell kialakítani.

Az érintett rendszert – a Legszűkebb funkcionalitás pont előírásaira tekintettel – úgy kell konfigurálni, hogy csak a működéshez elengedhetetlenül szükséges portok, protokollok és szolgáltatások legyenek engedélyezve.

A túlterheléses támadással kapcsolatos további védelmi intézkedések kidolgozása az üzemeltető feladata.

IV.7.3. A határok védelme

Az akkreditált informatikai rendszer határvédelmét tűzfalakkal kell biztosítani oly módon, hogy az érintett rendszer ne legyen közvetlenül elérhető az internet felől.
A tűzfal beállításaira az üzemeltető ad javaslatot az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelősének (IBF). Az üzemeltető informatikai vezetője és a Hivatal IBF-e közösen hagyja jóvá a javaslatot. A jóváhagyás után, a tűzfal végleges beállításait az üzemeltető kötelessége alkalmazni.
A tűzfalak felügyeletét folyamatosan biztosítani kell. Az üzemeltető kötelessége eljárásrendet készíteni és oktatni a rendszergazdáknak a tűzfal felügyeleti feladataival kapcsolatosan.

IV.7.4. Kriptográfiai kulcs előállítása és kezelése

Az akkreditált informatikai rendszerben a kriptográfiai kulcsokat a Hivatal kriptográfiai eljárásrendjének megfelelően kell előállítani és kezelni. Az üzemeltető kötelessége az eljárásrendben foglaltaknak megfelelően előállítani és kezelni a kriptográfiai eljárásokban használt kulcsokat. Amennyiben az akkreditált informatikai rendszer is alkalmas lesz kulcs előállítására és kezelésére, az alábbi szabályokat kell alkalmazni a Kriptográfiai védelem pont követelményein túl.

IV.7.4.1. Kriptográfiai kulcs létrehozása, inicializálása

A kriptográfiai eszközök inicializálása az eszköz típusától függően a következő folyamat mentén történik:

- Szoftveres kulcs esetén a kulcsok előállítása a rendszergazda, vagy az Információbiztonsági Felelős (IBF) feladata. A kulcsok létrehozása során meg kell róla győződni, hogy naprakész, megfelelően telepített és konfigurált szoftver- vagy hardverkomponensek kerülnek felhasználásra. Különös figyelmet kell fordítani az igénybe vett véletlenszám-generátor számára biztosított megfelelő entrópia-forrásról. A létrehozás során olyan környezet és tároló vehető igénybe, amelyen az átadás után biztosítható a biztonságos megsemmisítés.
- Hardveres kulcs esetén a gyártó ajánlásai és a Kriptográfiai védelem pont alapján kell létrehozni a kulcsot. Amennyiben a kulcs aktiválásához jelszó vagy PIN kód szükséges, úgy gondoskodni kell róla, hogy
    - A PIN/jelszó megfeleljen az akkreditált informatikai rendszert üzemeltető jelszókezelési szabályzatának;
    - A kezdeti PIN kódot/jelszót az átvevő megváltoztassa, vagy közvetlenül megadhassa.
- Hardveres kulcstárolás esetén gondoskodni kell róla, hogy a kulcstároló eszközről a magánkulcsok ne legyenek exportálhatóak.

A kulcsok bizalmassága természetükből fakadóan alapvető.

IV.7.4.2. Átadás

A létrehozás és átadás teljes folyamata során biztosítani kell, hogy a kriptográfiai eszközök tartalmát harmadik fél ne ismerhesse meg, arról másolatot, feljegyzést ne készíthessen. (Fájl megosztással szándékon kívül elérhetővé tett szoftveres kulcsok, felügyelet nélkül hagyott hardvereszközök kizárása, stb.)
Az átadott eszközök nyilvántartását az informatikai rendszert üzemeltető szervezet Információbiztonsági Felelős (IBF) végzi.

IV.7.4.3. Csere

A kriptográfiai kulcsok cseréje a létrehozás, átadás, megsemmisítés rendje szerint zajlik.

IV.7.4.4. Megsemmisítés

Amennyiben a megsemmisített kulcs olyan aszimmetrikus kulcspár része,

- amelyet azonosításra használnak, akkor a kulccsal való hozzáférést logikailag is meg kell szüntetni;

- amelyet hitelesítésre használnak, úgy a kulcsot a körülményektől függően vissza kell vonni, illetve a regisztrációját meg kell szüntetni.

A kulcs, kulcspár megsemmisítése során

- Hardveres kulcsok esetén az adathordozók kezelésére és megsemmisítésére vonatkozó előírásai;
- szoftveres kulcsok esetén az biztonságos adatmegsemmisítésre vonatkozó előírásai alkalmazandóak a kulcs minden előfordulási példánya esetén.

Amennyiben a kulcsról biztonsági másolat készül (DC, boríték, egyéb mentések), úgy a másolatok körültekintő megsemmisítéséről is gondoskodni kell.

A kulcsok megsemmisítését a rendszergazda végzi, erről jegyzőkönyvet vesz fel.

IV.7.5. Kriptográfiai védelem

Az akkreditált informatikai rendszer működtetése során csak olyan kriptográfiai megoldás alkalmazható, mely megfelel a 2015. évi CCXXII. Törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvény előírásainak, illetve a bizalmi szolgáltatások felügyeletét ellátó hatóság ajánlásainak és állásfoglalásainak.

Blokk titkosítók vonatkozásában az AES-128, AES-192, vagy AES-256, esetleg a három kulcsos TDEA módszerek egyikét kérjük használni. Sem a kétkulcsos TDEA, sem DES algoritmus alkalmazása nem elfogadható.

Digitális aláírás előállítására és ellenőrzésére legalább 2048 bit hosszú RSA, vagy legalább 224 bites ECDSA eljárások valamelyikét kérjük használni.

A szoftverben alkalmazott álvéletlen számok előállításához szükséges determinisztikus véletlen bit generátorban (Deterministic Random Bit Generator – DRBG) a HASH_DRBG, a HMAC_DRBG és a CTR_DRBG algoritmusok valamelyikét kérjük használni.

A kulcsegyeztetési (kulcscsere) folyamat (key agreement) egy olyan megoldás, amellyel a két kommunikációs fél között egy közös (szimmetrikus) kulcs előállítására kerül sor mindkét fél közreműködésével. Két sémát fogadnak el napjainkban erre a célra: a Diffie-Hellman (DH) és a Menezes-Qu_Vanstone (MQV) megoldásokat. Mindkettő alkalmazható véges testeken, vagy akár elliptikus görbéken. A kulcsegyeztetés folyamatának két lépése van: a DH, vagy MQV primitív használatával a megosztott kulcs előállítása, illetve a kulcs deriválási módszer (Key Derivation Method – KDM), amellyel egy vagy több további kulcs előállítható a megosztott kulcsból.

A véges testek fölött a DH és MQV paramétereinél legalább 2048 bites hosszúságot kérjük használni (len(p)≥2048 és len(q)≥224). Elliptikus görbék használata esetén az alábbi táblázatban lévő paraméterek használata kötelező, (len(n)<224 nem megengedett):

	EB	**EC**	**ED**	**EE**
Az n hossza	224—255	256—383	384—511	512+
a h koefficiens maximális hossza	14	16	24	32

Amennyiben a kulcsegyeztetési folyamatot és a kulcsok mozgatását RSA algoritmus használatával végzik, az RSA algoritmusnak legalább 2048 bites kulcsokat kell alkalmaznia.

A kulcscsomagolásra (key wrapping) kizárólag AES, vagy három-kulcsos TDEA algoritmusokat szabad használni.

További kulcsok generálásához (Key Derivation Function – KDF) csak HMAC alapú megoldás használható.

Lenyomatoló (hash) függvények előállítására csak az SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 és SHA-512/256) és SHA-3 (SHA3-224, SHA3-256, SHA3-384, and SHA3-512) családba tartozó algoritmusokat szabad használni. SHA-1 és korábbi (pl. MD4, MD5) hash függvények alkalmazása nem elfogadható.

Üzenet autentikációs kód (Message Authentication Code – MAC) az üzenetek sértetlenségének (az üzenet változatlan, eredeti formájában érkezett meg) és autentikusságának (a feladó valóban az, akinek hisszük) biztosítására alkalmazott eljárás. A MAC lehet hash alapú (HMAC) és blokk-titkosító alapú (CMAC, GMAC). HMAC esetében mind generálás mind verifikálás oldalon legalább 112 bit hosszú kulcsokat kell alkalmazni.

CMAC esetében csak AES és három-kulcsos TDEA alkalmazható mindkét oldalon. GMAC esetében az AES alkalmazása elfogadott generálás és verifikálás oldalon is.

IV.7.5.1. Jelszavak tárolása

A jelszó tárolása kapcsán is a fenti, hash függvényekre vonatkozó algoritmust kell alkalmazni. Az algoritmus maga legyen publikus (pl. nemzetközi szabványban leírt) és ne létezzen rá publikált sérülékenység. Javasolt a jelszótárolást a PBKDF 2.0 (Password-Based Key Derivation, RFC2898) alapján a NIST SP800-132 publikáció iránymutatásainak megfelelően megvalósítani, az alábbi függvény szerint: lenyomat = PBKDF2(CSHF, jelszó, salt, n, x), ahol a CSHF egy kriptográfiailag megbízható hash függvény (pl. SHA-256), a salt egy véletlen bitsorozat, az n pedig egy egész szám, amely a hash függvény n-szer egymás utáni használat definiálja (iteráció). Az x pedig a kívánt lenyomat hossza bitben.
Paraméterekkel szemben elvárt minimum elvárások: A salt legyen minimum 256 bit hosszú, az *n* legyen minimum 4096, illetve a kimeneti hossz (*x*) legyen minimum 256 bit.
Ajánlott algoritmusok: A PBKDF2 (RFC 2898) eljáráson alapuló bármely algoritmus használható, amelyek a fenti kritériumokat teljesítik. Javasolt már meglévő implementációk használata. Pl: bcrypt, scrypt.

IV.7.6. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)

Az akkreditált informatikai rendszerben a névfeloldási szolgáltatását úgy kell kialakítani, hogy a hiteles forrást biztosító DNS kiszolgáló (autoritatív DNS) kriptográfiai megoldással kiegészített biztonságos tranzakciókat valósítson meg a név/cím feloldási kérésekre adott hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozóan.
Az üzemeltető kötelessége gondoskodni arról, hogy az akkreditált informatikai rendszer minden komponense hiteles forrást biztosító DNS szolgáltatást nyújtson/használjon.

IV.7.6.1. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

Az akkreditált informatikai rendszerben biztosítani kell az érintett rendszer névfeloldási szolgáltatást biztosító infrastruktúrájának magas rendelkezésre állását, annak redundánssá alakításával.
A külső és a belső szerepköröket szét kell választani, azaz külön DNS kiszolgálót kell alkalmazni a belső hálózat kiszolgálására és külön kiszolgálónak kell ellátnia az internetes DNS kiszolgálókkal történő kapcsolattartást.

IV.7.7. A folyamatok elkülönítése

Az akkreditált informatikai rendszerben csak olyan (modern) operációs rendszerek és alkalmazások használhatóak, amelyek biztosítják az elkülönített végrehajtási tartomány fenntartását minden végrehajtó folyamat számára.
El kell különíteni az egyes üzleti folyamatokat az akkreditált informatikai rendszerben.