Az IT üzemeltető a Hivatal által használt elektronikus információs rendszerekkel kapcsolatos feladatai

Kivonat az Informatikai Biztonsági Szabályzatból

Az IT üzemeltető az informatikai rendszerelemek működési, üzemeltetési felelőssége körében az Informatikai Biztonsági Szabályzatban (továbbiakban: IBSZ) meghatározott alábbi biztonsági követelményekkel kapcsolatos feladatok végrehajtásáért felel. Az IBSZ-ben előírt feladatok végrehajtása a Hivatal jogszabályban meghatározott biztonsági besorolási szintjéhez tartozó biztonsági követelmények maradéktalan teljesítésének kötelező és elengedhetetlen feltétele, emiatt ezektől eltekinteni részben sem lehet! A feladatok végrehajtásának elmaradása vagy hiányos megvalósítása által okozott károk hátrányos jogkövetkezményei a tevékenységek ellátásáért felelős IT üzemeltetőt terhelik.

A dokumentumban az IBSZ vonatkozó fejezetszáma hivatkozásként, továbbá az ellátandó feladat értelmezéséhez szükséges mértékben az adott követelményhez tartozó szövegkörnyezet megjelenítésre került. Az IT üzemeltető által az adott követelménnyel kapcsolatban elvégzendő feladat típusa a követelményelemet követően felsorolva található. A meghatározott feladatok üzemeltetés szakmai szempontból több követelmény esetén átfedő, illetve megegyező tartalommal bírnak.

9 Cselekvési terv

A Hivatal a megvalósítandó biztonsági intézkedéseket és azok megvalósításának sorrendjét az elvárt biztonsági szint elérése céljából cselekvési tervben határozza meg.

A tervben foglalt feladatok végrehajtásában köteles minden érintett hivatali munkavállaló és az IT üzemeltető közreműködni. A tervben foglaltak végrehajtását az információbiztonsági felelős köteles – a tervben megállapított mérföldkövekhez, határidőkhöz igazodva – szükség szerint a Hivatal munkavállalói, az IT üzemeltető, illetve az egyéb közreműködők (pl.: szerződéses szolgáltató partnerek) bevonásával ellenőrizni, s annak eredményéről a Jegyzőt tájékoztatni, indokolt esetben a terv felülvizsgálatát, módosítását kezdeményezni, továbbá abban közreműködni.

IT üzemeltető feladata:

A cselekvési tervben foglalt feladatok végrehajtása, illetve közreműködés azok végrehajtásában.

10 Az Elektronikus információs rendszerek nyilvántartása

Az elektronikus információs rendszerek (továbbiakban: EIR) nyilvántartása kitöltéséhez az IT üzemeltető szakmai, módszertani támogatást biztosít.

IT üzemeltető feladata:

Nyilvántartás kitöltésének támogatása, tanácsadás.

14.1 Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

Az üzletmenet-folytonossági terv elkészítésében, végrehajtásában, rendszeres tesztelésében és felülvizsgálatában feladatellátása keretében részt vesz, illetve közreműködik az IT üzemeltető.

Az IT üzemeltető feladata gondoskodni arról, hogy minden, a tervben szereplő rendszer és erőforrás vonatkozásában rendelkezésre álljanak azok a dokumentált eljárások, amelyek alapján a helyreállítás elvégezhető.

Az IT üzemeltető feladata a visszaállítási eljárások dokumentált tesztelése, valamint változás esetén a mentési rend aktualizálása a 14.4 Az elektronikus információs rendszer mentései fejezetben előírtak szerint az alábbi rendszerességgel:

- új EIR bevezetése során;
- a mentési eljárásrendet érintő változás esetén (pl.: mentendő információk körének vagy a mentési gyakoriságnak a változása);
- az alkalmazott mentési technológia változása esetén;
- a rendelkezésre állási és visszaállítási követelmények változásakor;
- az előző pontokban felsorolt változások hiányában évente legalább egy alkalommal.

IT üzemeltető feladata:

Mentések dokumentálása, tesztelése, a dokumentáció aktualizálása.

14.2 Üzletmenet-folytonosságra vonatkozó eljárás

14.2.1 Esemény felismerése, jelzése

Amennyiben olyan esemény következik be, amely a Hivatal munkavégzéshez szükséges informatikai eszközöket, illetve rendszereit részben vagy teljesen működésképtelenné teszi, a Jegyzőt haladéktalanul értesíteni kell. Az értesítés az eseményt észlelő munkavállaló vagy IT üzemeltető feladata és kötelessége.

14.2.2 Döntés az erőforrás kiesés kezelésének módjáról

A Jegyző – szükség szerint az IT üzemeltetővel, központi vagy külső szolgáltatás esetén annak üzemeltetési kapcsolattartójával, illetve az információbiztonsági felelőssel konzultálva – a bekövetkezett erőforráskieséses állapot körülményeiről és hatásairól, az erőforráskiesés megszüntetésére vonatkozó intézkedések végrehajtásának becsült időtartamáról (helyreállítási idő) rendelkezésre álló információk mérlegelését követően dönt az esemény kezelési módjáról, amely lehet:

- kisebb hatású, az informatikai erőforrások szűk körét érintő vagy várhatóan rövid idejű erőforráskiesés esetén (pl.: olyan hibajelenség előfordulásakor, amely helyben – esetleg távoli segítségnyújtás igénybe vételével – kezelhető, mint például egy eszköz újraindítása) a szükséges intézkedés megtételének;
- az informatikai erőforrások széles körét vagy egészét érintő (vészhelyzet) esetén az üzletmenet-folytonossági tervben szereplő tartalék intézkedések, illetve helyreállító tevékenységek végrehajtásának elrendelése.

14.2.3 Vészhelyzet elhárítása, visszatérés a normál működési folyamathoz

A helyzet kezeléséről hozott döntésnek megfelelően a helyreállításban kompetens (pl.: IT üzemeltető) végrehajtja a szükséges intézkedést, majd annak eredményéről tájékoztatja a Jegyzőt és az információbiztonsági felelőst.

IT üzemeltető feladata:

Hibajelzések fogadása, biztonsági esemény jelzése, szakmai tanácsadás, biztonsági mentésből visszaállítás, rendszer helyreállítás.

14.4 Az elektronikus információs rendszer mentései

A biztonsági mentések konfigurálása és rendszeres végrehajtása a dokumentált mentési rend alapján (5. számú melléklet – Az elektronikus információs rendszerek mentése) az IT üzemeltető feladata és felelőssége. Az eseti biztonsági mentések, valamint a helyreállítási, illetve tesztelési célú visszatöltések végrehajtásáról az IT üzemeltető köteles a 5. számú melléklet – Az elektronikus információs rendszerek mentése dokumentumban meghatározott mentési napló tartalommal nyilvántartást vezetni.

IT üzemeltető feladata:

Biztonsági mentések beállítása, mentési megoldás működésének felügyelete, mentések dokumentálása – mentési napló vezetése.

14.5 Az elektronikus információs rendszer helyreállítása és újraindítása

Amennyiben a Hivatal által használt EIR-eket, rendszerelemeiket érintő hiba vagy biztonsági esemény kezelése biztonsági mentésből történő helyreállítási, illetve újraindítási tevékenységet igényel, azok végrehajtása az IT üzemeltető feladata és felelőssége. Kivételt képezhet ez alól a kisebb – nem kiszolgáló szintű – újraindítási feladatok végrehajtása (pl.: munkaállomás esetén), melyet – szükség szerint az IT üzemeltető szakmai támogatása mellett – az eszköz használatára feljogosított hivatali munkavállaló is végrehajthat.

IT üzemeltető feladata:

Szakmai tanácsadás, biztonsági mentésből visszaállítás, rendszer helyreállítás.

15.1 A biztonsági események figyelése

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező munkatársak és a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyek (pl.: IT üzemeltető) egyaránt kötelesek hibás működés vagy rendellenes esemény észlelése esetén jelezni. A jelzés formájától és tartalmától függően az esemény a kezelése során különböző eszkalációs szinteken kerülhet dokumentálásra. Elektronikus (pl.: email) jelzés esetén az észlelő, egyéb esetekben az IT üzemeltető, hatósági bejelentést igénylő biztonsági esemény kapcsán az információbiztonsági felelős által.

IT üzemeltető feladata:

Hibajelzések fogadása, biztonsági esemény jelzése.

15.2 A biztonsági események jelentése

A Hivatal által használt EIR-ek bármely rendszerelemének, hardver- illetve szoftver komponenseinek rendellenes vagy hibás működéséről, működési zavarairól vagy hibajelzéseiről lehetőség szerint elektronikus formában (email) – vagy ha az nem működik, akkor telefonon keresztül – minden munkavállaló köteles tájékoztatni az IT üzemeltetőt, aki biztonsági incidens gyanújának felmerülésekor köteles haladéktalanul tájékoztatni az információbiztonsági felelőst és a Jegyzőt.

IT üzemeltető feladata:

Hibajelzések fogadása, biztonsági esemény jelzése.

15.3 Segítségnyújtás a biztonsági események kezeléséhez

A biztonsági incidens kezelésének támogatását a 15.4 Biztonsági eseménykezelési terv fejezetben meghatározottak szerint, feladat- illetve felelősségi körének megfelelően az IT üzemeltető, illetve az információbiztonsági felelős végzi.

IT üzemeltető feladata:

Szakmai tanácsadás.

15.4 Biztonsági eseménykezelési terv

Az adott esemény biztonsági eseménnyé minősítését kérdéses esetben, illetve annak kiértékelése során az információbiztonsági felelős támogatja, illetve végzi el az eset összes körülményéről rendelkezésre álló információk alapján.

A biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez esetlegesen szükséges további információk (pl.: log fájlok) begyűjtésében az IT üzemeltető köteles közreműködni.

IT üzemeltető feladata:

Biztonsági események vizsgálatához információk – pl.: log fájlok – begyűjtése, továbbítása.

16.5 Fegyelmi intézkedések

A fegyelmi, illetve hatósági eljárásban felhasználni kívánt evidenciák begyűjtéséhez az információbiztonsági felelős szakmai iránymutatást, támogatást biztosít, az IT üzemeltető közreműködik, megőrzésükről a Jegyző köteles gondoskodni.

IT üzemeltető feladata:

Biztonsági események vizsgálatához információk – pl.: log fájlok – begyűjtése, továbbítása.

18.10 Be- és kiszállítás

A Hivatal a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint engedélyezi vagy tiltja a létesítménybe bevitt, illetve onnan kivitt információs rendszerelemeket. A be- és kiszállítás felügyeletét, figyelemmel kísérését a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személy felügyeletével megbízott munkatárs látja el, szakmai ellenőrzésében szükség szerint közreműködik az IT üzemeltető.

IT üzemeltető feladata:

Be- és kiszállításban érintett informatikai eszközök azonosítása, ellenőrzése – szakmai tanácsadás.

19.2 Az elektronikus információs rendszer kapcsolódásai

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a kapcsolódás szabályait, úgymint a rendszer kapcsolatait, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát a rendszer tulajdonosa határozza meg és dokumentálja. Új, saját fejlesztésű EIR használatba vétele esetén a Hivatal gondoskodik arról, hogy ugyanezen információk a rendszer dokumentációiban szerepeljenek. Saját üzemeltetésű EIR-ek esetében az IT üzemeltető felelős a meglévő rendszerdokumentációk fenti, esetleg hiányzó információkkal történő kiegészítéséért.

IT üzemeltető feladata:

Rendszerdokumentációk aktualizálása, vezetése.

19.3 Külső kapcsolódásokra vonatkozó korlátozások

A végrehajtható programok, script-ek (pl.: Java Applet, JavaScript, VB Script, CGI, stb.) letöltését, futtatásának lehetőségét, valamint web és alkalmazásba csomagolt ActiveX objektumok működését le

kell tiltani az internet böngésző programokban, továbbá gondoskodni kell arról, hogy a böngésző alkalmazás biztonsági frissítése rendszeresen megtörténjen.

Az internet csatlakozásra használt böngészőprogram biztonsági beállításait az IT üzemeltető a 23. Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni.

IT üzemeltető feladata:

Internet böngésző programok biztonsági beállításainak konfigurálása.

20.1 Rendszerbiztonsági terv

A rendszerbiztonsági terv felülvizsgálatában az információbiztonsági felelős jogosult – szükség szerint az IT üzemeltető bevonásával – közreműködni.

IT üzemeltető feladata:

Rendszerbiztonsági terv éves felülvizsgálatában közreműködés, szakmai tanácsadás).

21.3 A biztonsági teljesítmény mérése

A mérések végrehajtásában az IT üzemeltető, a Hivatal munkatársai, valamint a Hivatallal szerződéses jogviszonyban álló szervezetek (pl.: szolgáltatást nyújtók) kötelesek közreműködni, ahhoz információkat nyújtani.

IT üzemeltető feladata:

Szolgáltatás kiesések, leállások – rendelkezésre állás elvesztésével járó biztonsági események – időtartamáról éves összesítő adatok összegyűjtése, továbbítása.

22.1 Tesztelési, képzési és felügyeleti eljárások

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek esetében az EIR üzembe helyezését megelőzően, valamint az EIR, illetve rendszerelemeinek, működési környezetének jelentős megváltozása esetén a fejlesztő, illetve az IT üzemeltetető bevonásával gondoskodik az adott rendszer dokumentált funkcionális és biztonsági tesztelésének végrehajtásáról.

IT üzemeltető feladata:

Tesztelési feladatok végrehajtása.

23.1 Konfigurációkezelési eljárásrend

A konfiguráció megváltozását az IT üzemeltető minden esetben köteles dokumentálni a hardver és szoftver komponensekről vezetett nyilvántartásban (lásd: 23.8 Elektronikus információs rendszerelem leltár) illetve az érintett rendszer dokumentációjában.

IT üzemeltető feladata:

Konfigurációváltozások dokumentálása, rendszerdokumentációk és a rendszerelem leltár – vagy CMDB – aktualizálása.

23.3 A konfigurációváltozások felügyelete (változáskezelés)

A változtatás végrehajtása az engedély birtokában a kijelölt felelős (pl.: IT üzemeltető) feladata. A változtatást az IT üzemeltető hardver és szoftver komponensek esetében a 23.8 Elektronikus információs rendszerelem leltárban, beállítások módosítása esetén az érintett rendszer dokumentációjában köteles rögzíteni.

IT üzemeltető feladata:

Konfigurációváltozások dokumentálása, rendszerdokumentációk és a rendszerelem leltár – vagy CMDB – aktualizálása.

23.4 Előzetes tesztelés és megerősítés

Hardver meghibásodás miatt szükséges rendszerelem csere esetében a beépítésre kerülő új hardverelem műszaki megfelelőségének vizsgálata az IT üzemeltető feladata. Karbantartás, illetve hibajavítás céljából kizárólag olyan hardverelem építhető be, amely a használt EIR-ek ismert kompatibilitási és konfigurációs igényeinek megfelel.

IT üzemeltető feladata:

Új hardver elemek műszaki megfelelőségének vizsgálata a rendelkezésre álló kompatibilitási információk, rendszerdokumentációk alapján.

23.6 Konfigurációs beállítások

A beállítások elvégzése, a konfigurációs követelményekről rendelkezésre álló rendszer dokumentációk alapján az IT üzemeltető feladata. Amennyiben a konfiguráció során a meghatározott beállításokhoz képest eltérést tapasztal, úgy azt köteles a 23.3 A konfigurációváltozások felügyelete (változáskezelés) fejezetben előírtak szerint jelezni, valamint a rendszer dokumentációjában rögzíteni.

IT üzemeltető feladata:

Konfigurációs beállítások végrehajtása, változások dokumentálása, rendszerdokumentációk és a rendszerelem leltár – vagy CMDB – aktualizálása.

23.7 Legszűkebb funkcionalitás

A Hivatal a saját fejlesztésű és általa üzemeltetett, a felügyelete, irányítása alatt lévő EIR-ek konfigurációs beállításait a legszűkebb funkcionalitás elvének megfelelően, a nem szükséges funkciók, portok, protokollok, szolgáltatások korlátozásával, illetve tiltásával határozza meg és dokumentálja. A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott EIR használatához szükséges és elégséges konfigurációs beállításokat.

A beállítások végrehajtását az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni.

IT üzemeltető feladata:

Konfigurációs beállítások végrehajtása, változások dokumentálása, rendszerdokumentációk aktualizálása.

23.8 Elektronikus információs rendszerelem leltár

A Hivatal által használt EIR-ek rendszerelemeiről, a hardver és szoftver komponensekről az IT üzemeltető köteles naprakész nyilvántartást vezetni. A nyilvántartásnak minimálisan a 10. számú melléklet – Elektronikus információs rendszerelem leltár mellékletben meghatározott tartalommal kell rendelkeznie, s biztosítania kell a nyilvántartott rendszerelemek egyértelmű beazonosíthatóságát.

A nyilvántartás elektronikus formában (pl.: konfigurációkezelési adatbázis), illetve automatizált változásfelügyeleti megoldással aktualizálható módon egyaránt vezethető, amennyiben képes biztosítani a komponensek változásainak időbeni visszakereshetőségét.

IT üzemeltető feladata:

Rendszerelem nyilvántartás, leltár – vagy CMDB – vezetése, aktualizálása.

23.9 A szoftverhasználat korlátozásai

Az IT üzemeltető feladata ellenőrizni a Hivatal informatikai rendszereiben telepített és futtatott programokat és alkalmazásokat, a mennyiségi licencekkel védett szoftverek használatát a 10. Az elektronikus információs rendszerek nyilvántartásában, illetve kereskedelmi szoftver esetén a felhasználásra vonatkozó szerződésben szereplő engedélyezett licence szám alapján, valamint az állomány megosztásokat az esetlegesen szerzői joggal védett tartalmak jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására irányuló tevékenységek szűrése céljából.

Nem engedélyezett tevékenység vagy szoftverhasználat észlelése esetén az IT üzemeltető köteles a Jegyzőt haladéktalanul tájékoztatni, valamint az utasításának megfelelően a szükséges intézkedéseket (pl.: nem engedélyezett szoftver vagy jogvédett tartalom eltávolítása) megtenni.

IT üzemeltető feladata:

Telepített programok, szoftverhasználat, illetve állomány megosztások rendszeres ellenőrzése; jogvédett tartalmak, nem jogtiszta szoftverek eltávolítása.

23.10 A felhasználó által telepített szoftverek

A munkaállomásokra telepített szoftvereket az IT üzemeltető ellenőrzi a 23.9 A szoftverhasználat korlátozásai fejezetben meghatározottak szerint.

IT üzemeltető feladata:

Telepített programok, szoftverhasználat, illetve állomány megosztások rendszeres ellenőrzése; jogvédett tartalmak, nem jogtiszta szoftverek eltávolítása.

24.1 Rendszer karbantartási eljárásrend

A Hivatal által használt EIR-ek folyamatos működésének biztosítása, rendelkezésre állásának megőrzése érdekében az IT üzemeltető feladata az informatikai eszközök, a rendszerelemek hardver, illetve szoftver komponenseinek rendszeres és dokumentált karbantartásáról, szükség szerinti javításáról gondoskodni.

IT üzemeltető feladata:

Informatikai eszközök karbantartása, javítása – végrehajtás, illetve a karbantartás, javítás megszervezése.

24.2 Rendszeres karbantartás

A karbantartásról az IT üzemeltető az adott rendszerelemre vonatkozó gyártói ajánlásoknak megfelelő módon és rendszerességgel köteles gondoskodni.

A tervezett karbantartási, illetve a szükséges javítási feladatok végrehajtásáról az IT üzemeltető köteles a Jegyzőt előzetesen tájékoztatni. A Jegyző a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján dönt a tevékenység jóváhagyásáról.

Adathordozót is tartalmazó rendszerelem (eszköz) esetén az elszállítás előtt az IT üzemeltető feladata az adathordozón található adatok és információk szükség szerinti eseti biztonsági mentéséről a 5. számú melléklet – Az elektronikus információs rendszerek mentése dokumentumban meghatározottak szerint, s az adathordozóról történő visszaállíthatatlan módú törléséről gondoskodni.

A Jegyző a Hivatal munkatársainak közreműködésével – indokolt esetben az információbiztonsági felelős bevonásával – ellenőrzi, hogy a rendszerelem, illetve az EIR a karbantartási vagy javítási tevékenységek után is megfelelően működik-e. A Jegyző és az információbiztonsági felelős jogosult az IT üzemeltetőtől minden olyan információt (hozzáférést, adatot, dokumentációt, stb.) bekérni, az IT üzemeltető pedig köteles biztosítani, amely a funkcionális, illetve biztonsági ellenőrzés végrehajtásához szükséges.

A karbantartási, illetve javítási tevékenységekről az IT üzemeltető köteles nyilvántartást vezetni, s ezzel kapcsolatban keletkező dokumentációk hozzáférhetőségét azok megjelenési formájától függően a Hivatal számára biztosítani a 4. Dokumentumvédelem fejezetben meghatározott szabályok szerint.

IT üzemeltető feladata:

Informatikai eszközök karbantartása – végrehajtás, illetve a karbantartás, javítás megszervezése. Adatok mentése, adathordozó törlése. Javított eszköz működésének ellenőrzése, tesztelése. Karbantartási, javítási tevékenységek nyilvántartása.

25.2 Hozzáférés az adathordozókhoz

A munkavégzéshez a Hivatal által biztosított mobil adattároló vagy beépített adathordozót tartalmazó mobil eszközön munkavégzéshez kapcsolódó információkat az adathordozó típusának megfelelően lehetőség szerint fájl- vagy tárolószintű titkosítással ellátva kell tárolni. Az eszköz biztonságát – amennyiben technológiai oldalról támogatott – további hozzáférés védelmi megoldás (pl.: jelszó, PIN kód, stb.) alkalmazásával is biztosítani kell.

A kriptográfiai védelem kialakításában és beállításában az IT üzemeltető feladata közreműködni, a titkosításhoz használt kulcsok, egyedi azonosítók és hitelesítő eszközök (pl.: jelszó) biztonságos kezelése és megőrzése az eszköz, illetve adathordozó használatára jogosult feladata és felelőssége.

Adathordozó előállítására alkalmas eszköz, berendezés (pl.: nyomtató) a Hivatal nyitvatartási idejében az ügyfelek és látogatók által hozzáférhető, felügyelet nélkül lévő helyiségbe nem helyezhető el. Kivéve, ha az adott eszköz képes felügyelt nyomtatást biztosítani, s beállításra kerül rajta, hogy nyomtatási feladat kizárólag a nyomattulajdonos helyi hitelesítését követően hajtható végre. Az eszköz konfigurálása, a beállítások dokumentálása az IT üzemeltető feladata.

IT üzemeltető feladata:

Mobil adattároló, mobil eszköz fájl- vagy tárolószintű titkosításának beállítása. Nyomtató helyi hitelesítés kikényszerítésének – amennyiben alkalmas rá az eszköz – konfigurálása, dokumentálása.

25.3 Adathordozók törlése

Az IT üzemeltető feladata az adathordozó típusának megfelelő helyreállíthatatlanságot biztosító törlési technikát (pl.: többszörös felülírás, roncsolás, stb.) alkalmazva törölni a Hivatal által használt EIR-ek és

a munkavégzéshez a Hivatal által biztosított mobil eszközök beépített adathordozóit, továbbá a mobil elektronikus adathordozókat azok leselejtezése vagy újrafelhasználásra való kibocsátása előtt.

Amennyiben javítási, karbantartási célból adathordozót is tartalmazó rendszerelem (eszköz) ideiglenesen kikerül a Hivatal felügyelete alól, a kiszállítás előtt az IT üzemeltető feladata az adathordozón található adatok és információk szükség szerinti eseti biztonsági mentéséről, s az adathordozóról történő visszaállíthatatlan módú törléséről gondoskodni.

IT üzemeltető feladata:

Adathordozók törlése, adatok biztonsági mentése.

25.4 Adathordozók használata

A nem a Hivatal tulajdonát képező, idegen adathordozó vagy mobil eszköz csatlakoztatását megelőzően az IT üzemeltető feladata az adathordozó megbízhatóságának ellenőrzése (pl.: vírusellenőrzés).

IT üzemeltető feladata:

Idegen adathordozó vírusellenőrzése – akár automatizáltan, megfelelő konfigurációs beállítással.

26.1 Azonosítási és hitelesítési eljárásrend

A munkavégzéshez szükséges azonosítók, felhasználói fiókok létrehozását és konfigurálását, a jogosultságok beállítását a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyezi, s az IT üzemeltető hajtja végre.

IT üzemeltető feladata:

Felhasználói fiókok létrehozása, adminisztrálása; hozzáférések, jogosultságok beállítása.

26.3 Hálózati hozzáférés privilegizált fiókokhoz

Új EIR fejlesztése, bevezetése során a Hivatal a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz (pl.: rendszer adminisztrátor, rendszergazda) való hálózaton keresztüli hozzáféréshez többtényezős hitelesítés alkalmazását követeli meg.

A meglévő, általa használt EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor a Hivatal gondoskodik a többtényezős hitelesítés kialakításáról a privilegizált hálózati hozzáférésekhez. Ha az adott rendszerben a többtényezős hitelesítés nem oldható meg, akkor megtiltja a hálózati hozzáférést a privilegizált felhasználói számára. A tiltás beállítása és a rendszer dokumentációjában történő rögzítése a 23.6 Konfigurációs beállítások fejezetben előírtak szerint az IT üzemeltető feladata. Amennyiben az adott EIR-ben sem a többtényezős hitelesítés megvalósítására, sem pedig a tiltás konfigurálására nincs lehetőség, a Hivatal gondoskodik a rendszer követelményeknek megfelelő, tervezett kiváltásáról.

IT üzemeltető feladata:

Egytényezős hitelesítést alkalmazó privilegizált hálózati hozzáférések tiltása, dokumentálása.

26.4 Azonosító kezelés

A munkaállomásokon, szerver kiszolgáló gépeken, valamint a Hivatal kezelésében, felügyelete alatt álló informatikai eszközökön (pl.: hálózati eszközök, nyomtatók, stb.) a helyi, illetve címtár használata esetén a tartományi felhasználói azonosítók létrehozása, hozzárendelése a meghatározott egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz, továbbá az azonosítók adminisztrálása, nyilvántartása az IT

üzemeltető feladata. A Hivatal által használt EIR-ek esetében, amennyiben azok önálló azonosítási megoldással rendelkeznek és a felhasználói azonosítók kezelése a Hivatal hatáskörébe tartozik, akkor azok kezelése az erre feljogosított szerepkört (pl.: alkalmazás adminisztrátor, tenant admin, stb.) betöltő, a Jegyző által e feladat végrehajtásával megbízott munkatárs feladata.

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon a felhasználó 15 perc időtartamú inaktivitása esetén azonosítóját le kell tiltani (pl.: számítógép zárolása, számítógép üresjárati korlátja). A munkaállomás újbóli használatát ismételt hitelesítéshez kell kötni. Az ezekhez szükséges beállítások végrehajtását az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni.

Új EIR fejlesztése, bevezetése során a Hivatal az azonosítók kezelésével kapcsolatban megköveteli, hogy az paraméterezhető módon, meghatározott időtartamig legyen képes megakadályozni az azonosító ismételt felhasználását, továbbá meghatározott időtartamú inaktivitás esetén tiltsa le az azonosítót. Meglévő EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor az IT üzemeltető feladata ennek dokumentált konfigurálása.

IT üzemeltető feladata:

Felhasználók adminisztrálása, nyilvántartása, dokumentálása. Munkaállomások biztonsági beállításainak konfigurálása: inaktív felhasználói azonosítók időkorlátos tiltása, stb.

26.5 A hitelesítésre szolgáló eszközök kezelése

A hitelesítésre szolgáló eszközök kiosztását, továbbá a felhasználásának megfelelő jogosultságok beállítását 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyezi, s a 26.4 Azonosító kezelés fejezetben előírtak szerint az azonosítók kezelésével megbízott (IT üzemeltető, tenant admin, stb.) hajtja végre.

A felhasználói jelszavakat tilos papír alapon, felírva tárolni! Kivételt képeznek ez alól a privilegizált hozzáférésekhez tartozó azonosítók és jelszavaik, melyeket rendelkezésre állásuk folyamatos biztosítása érdekében az azonosító kezelője (pl.: IT üzemeltető) köteles létrehozásuk és minden módosításuk alkalmával egy példányban beazonosítható módon dokumentálni, s azt átadni a Jegyző számára, aki gondoskodik azok biztonságos megőrzéséről és kezeléséről (lezárt borítékban, páncélszekrényben).

Az internetkapcsolaton keresztül elérhető EIR-ek, illetve rendszerelemeik esetében az internet böngészőprogramok beépített kényelmi funkciójának, a bejelentkezési adatok tárolásának (pl.: automatikus kiegészítés, felhasználói jelszavak megjegyzése) a használata tilos, a funkciót ki kell kapcsolni!

A felhasználói jelszavakkal kapcsolatos szabályok (jelszó házirend, böngésző program, stb.) beállítását az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírtak szerint köteles elvégezni. Felhasználói fiók, hozzáférés, illetve jogosultság változás esetén a hitelesítő eszköz módosításáról a 16.1 Személybiztonsági feltételek fejezetben meghatározottak szerint az IT üzemeltető feladata gondoskodni.

A privilegizált hozzáférések alapértelmezett jelszavait (pl.: hálózati eszközök esetében) az IT üzemeltető köteles a rendszerelem első konfigurációja, telepítése alkalmával megváltoztatni és dokumentálni, valamint a beállított hozzáférés adatait a Jegyző rendelkezésére bocsátani.

IT üzemeltető feladata:

Kezdeti jelszavak, jogosultságok beállítása. Alapértelmezett admin jelszavak megváltoztatása. Privilegizált hozzáférések adatainak dokumentálása, átadása. Jelszó házirend beállítása.

26.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A Hivatal által használt EIR-ekhez, illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb szerződéses, munkavégzésre irányuló jogviszonyban álló személyek számára, tevékenységük nyomon követhetőségének biztosítása érdekében minden esetben egyedi azonosítót képez, s ez alapján hitelesíti őket. Az azonosítók létrehozása és a használatukhoz szükséges hitelesítő eszközök kiosztása a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján, a Jegyző engedélyével, a 26.4 Azonosító kezelés fejezetben előírtak szerint az azonosítók kezelésével megbízott (IT üzemeltető, tenant admin, stb.) feladata.

IT üzemeltető feladata:

Felhasználók adminisztrálása, nyilvántartása, dokumentálása.

27.1 Hozzáférés ellenőrzési eljárásrend

Az információbiztonsági felelős jogosult a hozzáférések, illetve felhasználói fiókok kezelésével kapcsolatos beállítások és tevékenységek ellenőrzésére, illetve felülvizsgálati tevékenysége során – minimum éves rendszerességgel – auditálja azt. Az eseti, illetve rendszeres ellenőrzések lefolytatásában, a felülvizsgálatban az IT üzemeltető köteles közreműködni, ahhoz információkat nyújtani.

IT üzemeltető feladata:

Felülvizsgálatában közreműködés, hozzáférésekre vonatkozó információk összegyűjtése, átadása.

27.2 Felhasználói fiókok kezelése

A Hivatal által használt EIR-ekben, valamint az azokhoz hozzáférést biztosító munkaállomásokon a hivatali munkavégzéshez szükséges azonosítók, felhasználói fiókok létrehozását, a jogosultságok beállítását, továbbá ezek módosítását a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás alapján a Jegyző engedélyezi, s a 26.4 Azonosító kezelés fejezetekben meghatározottak szerint kijelölt felelős hajtja végre.

A fiók kezelőjét a Jegyző köteles értesíteni, amennyiben az adott

- felhasználói fiókra már nincs szükség;
- felhasználó kilépett vagy áthelyezésre került;
- EIR használata vagy az ehhez szükséges ismeretek megváltoztak.

IT üzemeltető feladata:

Felhasználók adminisztrálása, nyilvántartása, dokumentálása.

27.3 Hozzáférés ellenőrzés érvényesítése

A Hivatal által használt EIR-ek esetében a hivatali munkavégzéshez szükséges azonosítók, felhasználói fiókok létrehozását, a jogosultságok beállítását, továbbá ezek módosítását szintén minden esetben a Jegyző engedélyezi, s ez alapján a 26.4 Azonosító kezelés fejezetben meghatározottak szerint kijelölt felelős hajtja végre. A jóváhagyott jogosultságok érvényesítése az azonosítás és hitelesítés során történik meg.

A Hivatal által használt EIR-ekhez hozzáférést biztosító, a Hivatal által felügyelt kiszolgálók és munkaállomások biztonsági beállításait az IT üzemeltető jogosult módosítani.

IT üzemeltető feladata:

Munkaállomások, kiszolgálók adminisztrálása.

27.4 Sikertelen bejelentkezési kísérletek

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások és kiszolgálók biztonsági beállításait (fiókzárolási házirend) az IT üzemeltető a 23.6 Konfigurációs beállítások fejezetben előírt eljárás szerint, az alábbi szabályoknak megfelelően köteles végrehajtani:

- a felhasználó 3 egymást követő sikertelen bejelentkezési kísérlete esetén a munkaállomás automatikusan zárolja a felhasználói fiókot (pl.: fiókzárolási küszöb);
- a fiók zárolása automatikusan 30 perc elteltével kerüljön feloldásra (pl.: fiókzárolás időtartama, fiókzárolási számlázó nullázása).

IT üzemeltető feladata:

Munkaállomások, kiszolgálók biztonsági beállításainak adminisztrálása, dokumentálása.

27.5 A rendszerhasználat jelzése

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon az IT üzemeltető feladata a 23.6 Konfigurációs beállítások fejezetben előírt eljárás szerint az alábbi tartalmi elemekkel bíró, a rendszerhasználat jelzésére vonatkozó üzenet (interaktív bejelentkezési üzenet) beállítása:

- Ön «Hivatal_névelős_neve» rendszerét használja;
- a rendszer használatát figyelhetik, rögzíthetik, naplózhatják;
- a rendszer jogosulatlan használata tilos és büntetőjogi vagy polgárjogi felelősségre vonással jár;
- a bejelentkezéssel fentieket tudomásul veszi és azokhoz hozzájárul.

Új EIR fejlesztése, bevezetése során a Hivatal a rendszerhasználat jelzésével kapcsolatban fenti szabályoknak történő megfelelést követeli meg. Meglévő EIR-ek esetében, amennyiben az a hatáskörébe, felügyelete alá tartozik és technológiai szempontból megvalósítható, akkor az IT üzemeltető feladata ennek dokumentált konfigurálása.

IT üzemeltető feladata:

Munkaállomások, kiszolgálók biztonsági beállításainak adminisztrálása, dokumentálása.

27.6 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az azonosítás és hitelesítés nélküli hozzáférést vagy anonim bejelentkezést lehetővé tevő beépített fiókok (pl.: vendég) letiltásáról az IT üzemeltető köteles gondoskodni.

IT üzemeltető feladata:

Munkaállomások, kiszolgálók biztonsági beállításainak adminisztrálása, dokumentálása. Vendég fiókok letiltása.

27.8 Vezeték nélküli hozzáférés

A Hivatal vezeték nélküli hálózati beállításainak kezelése, dokumentálása az IT üzemeltető feladata. A beállítások ellenőrzésére az információbiztonsági felelős felügyeleti tevékenysége keretében jogosult.

IT üzemeltető feladata:

WIFI csatlakozás konfigurálása, dokumentálása, rendszerdokumentáció aktualizálása – változás esetén.

27.9 Mobil eszközök hozzáférés ellenőrzése

A Hivatal által a munkavégzéshez biztosított, a Hivatal tulajdonát képező mobil eszközök használatba vétele előtt az IT üzemeltető köteles gondoskodni a 25. Adathordozók védelme és a 28.3 Kártékony kódok elleni védelem fejezetekben előírt védelmi funkciók, valamint a titkosított adatátvitel megvalósításához szükséges alkalmazások (pl.: VPN) beállításáról.

IT üzemeltető feladata:

Titkosítás konfigurálása.

27.11 Nyilvánosan elérhető tartalom

A közzétételre alkalmazott kiszolgálón a nyilvánosan hozzáférhető információk elhelyezésében, törlésében az IT üzemeltető, illetve a honlap adminisztrálásával megbízott felelős köteles közreműködni.

IT üzemeltető feladata:

Weboldal adminisztrálása – amennyiben az IT üzemeltető feladatkörébe tartozik.

28.2 Hibajavítás

A Hivatal informatikai infrastruktúrájába, üzemeltetés felügyeleti hatáskörébe tartozó rendszerelemek hibáinak javításáról, illetve rendszeres karbantartásáról az IT Üzemeltető a 23. Konfigurációkezelés és a 24.1 Rendszer karbantartási eljárásrend fejezetekben előírtak szerint köteles gondoskodni.

A 28.5 Biztonsági riasztások és tájékoztatások fejezet alapján az információbiztonsági felelős által a biztonságkritikus szoftverekre, frissítéseikre vonatkozóan jelzett tevékenységek dokumentált végrehajtása az IT üzemeltető feladata és felelőssége.

IT üzemeltető feladata:

Biztonsági frissítések, security patch-ek, új firmware verziók telepítése, a végrehajtás dokumentálása.

28.3 Kártékony kódok elleni védelem

A Hivatal minden interneteléréssel rendelkező munkaállomásán és a Hivatal által munkavégzés céljára biztosított mobil infokommunikációs eszközén (pl.: laptop, tablet, telefon, stb.) víruskereső és vírusirtó funkcionalitással bíró védelmi szoftvert kell működtetni, amelynek telepítése, biztonsági beállításainak konfigurálása az IT üzemeltető feladata és felelőssége.

A megfelelő védelmi szoftver kiválasztása az IT üzemeltető feladata, a működési feltételek (pl.: szükséges licencek) biztosításáról a Hivatal köteles gondoskodni. Az információbiztonsági felelős felülvizsgálati tevékenysége keretében ellenőrzi és javaslatot tehet a kártékony kódok elleni védelemre alkalmazott megoldás cseréjére, kiváltására, amennyiben az nem képes megfelelően biztosítani a Hivatal által használt EIR-ek egyenszilárd és kockázatokkal arányos védelmét (pl.: kritikus sérülékenységei válnak ismertté, gyártói támogatása nem biztosítja valamely elvárt funkcionalitást vagy megszűnik, stb.).

Minden munkavállaló köteles a védelmi szoftver által megjelenített riasztásról az IT üzemeltetőt haladéktalanul értesíteni.

Az IT üzemeltető feladata a védelmi szoftver által generált riasztások kivizsgálása, s indokolt esetben a 15. A biztonsági események kezelése fejezetben meghatározottak szerint a Jegyző, illetve az információbiztonsági felelős tájékoztatása.

Vírusfertőzés tényének fennállása esetén az IT üzemeltető jelzése nyomán a Jegyző kihirdeti a vírusriadó állapotot, erről tájékoztatja az információbiztonsági felelőst és a hivatali munkatársakat.

A helyreállítási tevékenység keretében az IT üzemeltető gondoskodik – szükség szerint a hivatali munkavállalók közreműködésével - a fertőzött eszköznek a hivatali belső hálózatról történő leválasztásáról, a vírusfertőzés megszüntetéséről, a veszélyeztetett munkaállomások (pl.: azonos alhálózatban lévő gépek), rendszerelemek vírusellenőrzéséről illetve a vírus eltávolítását követően adatvesztés vagy sérülés esetén az állományok, illetve konfigurációk mentésből történő visszaállításáról.

A sikeres helyreállítást követően az IT üzemeltető jelzése nyomán a Jegyző hirdeti ki a vírusriadó állapot, valamint az annak időtartama alatt esetlegesen bevezetett ideiglenes védelmi intézkedések alkalmazásának megszüntetését.

IT üzemeltető feladata:

Vírusvédelmi szoftver jelzéseinek kivizsgálása, jelzések fogadás, vírusfertőzés megszüntetésével, helyreállítással kapcsolatos feladatok végrehajtása.

28.4 Az elektronikus információs rendszer felügyelete

Az EIR-ek felügyeletével kapcsolatban rendelkezésre álló felügyeleti információkhoz történő hozzáférést az információbiztonsági felelős számára, annak éves felülvizsgálati tevékenységéhez, illetve eseti jelleggel a bekövetkezett biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez az IT üzemeltető, illetve az adott EIR felügyeleti információihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl.: tenant admin, honlap adminisztrátora, stb.) köteles biztosítani.

IT üzemeltető feladata:

Felülvizsgálatában közreműködés, információk – pl.: log fájlok –információk összegyűjtése, átadása.

29.1 Naplózási eljárásrend

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások, kiszolgálók és a felügyelete alá tartozó további (pl.: hálózati) eszközök esetében az IT üzemeltető, illetve az adott EIR vagy rendszereleme naplózási beállításaihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl.: tenant admin, honlap adminisztrátora, stb.) jogosult és köteles a jelen fejezetben meghatározott naplózási beállításokat a 23. Konfigurációkezelés fejezetben előírt szabályok szerint végrehajtani.

IT üzemeltető feladata:

Naplózás konfigurálása.

29.4 Napló tárkapacitás

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások, kiszolgálók és a felügyelete alá tartozó további (pl.: hálózati) eszközök konfigurálását az IT üzemeltető úgy kell, hogy elvégezze, hogy azokon a naplóinformációk helyi eseménynaplóban történő rögzítéséhez, a naplóállományok helyben történő tárolásához szükséges tárkapacitás rendelkezésre álljon a 29.9 A naplóbejegyzések megőrzése fejezetben meghatározott időtartamig. (30 nap!)

IT üzemeltető feladata:

Naplózás konfigurálása.

29.6 Naplóvizsgálat és jelentéskészítés

Az IT üzemeltető köteles a naplóbejegyzések felülvizsgálatát, elemzését a nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából legalább havi rendszerességgel elvégezni, s amennyiben problémát tapasztal, akkor az információbiztonsági felelőst tájékoztatni.

A 28.5 Biztonsági riasztások és tájékoztatások fejezetben foglaltak szerint, fokozott kockázatra utaló jelzés esetén az információbiztonsági felelős kérheti a naplózandó események körének kibővítését, a naplóbejegyzések vizsgálatának gyakrabban történő végrehajtását, illetve a rendelkezésre álló felügyeleti információkhoz történő hozzáférés biztosítását, melyben az IT üzemeltető, illetve az adott EIR felügyeleti információihoz hozzáféréssel rendelkező, azok kezelésével megbízott (pl.: tenant admin, honlap adminisztrátora, stb.) köteles közreműködni.

IT üzemeltető feladata:

Naplóinformációk havi, rendszeres elemzése; eredményének jelzése. Naplózás konfigurálása.

29.7 Időbélyegek

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások, kiszolgálók és a felügyelete alá tartozó további (pl.: hálózati) eszközök esetében annak érdekében, hogy azok rendszerórái folyamatosan szinkronban legyenek az IT üzemeltető feladata minden eszközre egységesen megbízható, központi időforrás alkalmazásának konfigurálása.

IT üzemeltető feladata:

Munkaállomások, kiszolgálók idő szinkron beállításainak adminisztrálása.

29.9 A naplóbejegyzések megőrzése

A Hivatal által használt, általa üzemeltetett, illetve felügyelete alá tartozó EIR-ek és azon rendszerelemeik esetében, amelyeknél a naplóinformációk kezelése a hatáskörébe tartozik, a biztonsági események utólagos kivizsgálásának biztosítása érdekében a naplóbejegyzések megőrzéséről a Hivatal az alábbiak szerint gondoskodik:

a) a naplóinformációkat helyi eseménynaplóban rögzítő EIR-ek és elemeik esetében a naplózási beállításokat az IT üzemeltető úgy kell, hogy konfigurálja, hogy a naplóállományok helyben tároltan – amennyiben jogszabály a megőrzési időt nem korlátozza - legalább 30 napra visszamenőleg rendelkezésre álljanak;
b) amennyiben a helyi eseménynapló beállításai, illetve a rendelkezésre álló, e célra dedikáltan fenntartható tároló kapacitás a naplózandó események mennyisége miatt ezt nem teszi lehetővé, abban az esetben a naplózást archiválásra kell beállítani (az idő előtti felülírás elkerülése érdekében), s gondoskodni szükséges az archív naplóállományok legalább 30 napig történő megőrzéséről (hálózati- vagy külső tárolón, illetve a mentési eljárás keretein belül a mentési gyakoriság figyelembe vételével), ha jogszabály a megőrzési időt nem korlátozza;
c) központi naplógyűjtő rendszer alkalmazása esetén, amennyiben a gyűjtés automatizált módon, online vagy ütemezett rendszerességgel biztosított, a helyi (számítógépen történő) naplóállomány archiválás mellőzhető, a naplógyűjtő rendszerben kell – amennyiben jogszabály a megőrzési időt nem korlátozza – legalább 30 napig megőrizni a naplóbejegyzéseket.

IT üzemeltető feladata:

Naplózás konfigurálása.

30.3 A határok védelme

A Hivatal a belső hálózat védelmének biztosítása érdekében határvédelmi megoldást (tűzfal) alkalmaz a hálózati forgalom felügyeletére, irányítására. A határvédelmi eszköznek minimálisan az alábbi biztonsági funkciókat kell ellátnia:

- végezzen címfordítást a belső, nem nyilvános és a külső hálózati címek között;
- a 23.7 Legszűkebb funkcionalitás fejezetben előírtakkal összhangban alapból tiltania kell és csak kivételként engedélyezhet bármely hálózati forgalmat;
- csak a protokoll és port szinten jóváhagyott kommunikációt engedheti át;
- utólag visszakereshető módon, szabványos formátumban naplózza a sikeres, engedélyezett, illetve a blokkolt hálózati forgalom leíró adatait (forrás-, cél cím; port, protokoll, időpont, stb.).

A határvédelmi eszköz adminisztrálása a védett, belső hálózatból, illetve távoli hozzáférés esetén csak biztonságos kommunikációs csatornán keresztül engedélyezett.

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomások és kiszolgálók kizárólag a határvédelmi eszközön felügyelt interfészeken keresztül kapcsolódhatnak külső hálózatokhoz vagy külső elektronikus információs rendszerekhez (lásd: 19.3 Külső kapcsolódásokra vonatkozó korlátozások).

Amennyiben a Hivatal nyilvánosan hozzáférhető rendszerelemeket (pl.: web kiszolgáló szervert) üzemeltet, azt a belső hivatali hálózattól elkülönített, logikailag szeparált alhálózatban helyezi el, hálózati irányonként – belső, illetve külső – külön fizikai csatoló interfészekkel. A rendszerelemek, valamint a logikai elválasztás konfigurálása az e célra szolgáló, menedzselhető hálózati eszközön az IT üzemeltető feladata.

IT üzemeltető feladata:

Menedzselhető hálózati eszközök konfigurálása.

30.6 Együttműködésen alapuló számítástechnikai eszközök

A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon kizárólag abban az esetben engedélyezett együttműködésen alapuló számítástechnikai eszközök (pl.: kamera, mikrofon) használata, amennyiben a hivatali munkavégzés, illetve az adott EIR használata (pl.: kommunikáció) céljából indokolt. A funkciót biztosító eszközzel (alkalmazás, szoftver) szembeni követelmény, hogy közvetlen kijelzést nyújtson a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

Az alkalmazni kívánt eszköz megfelelőségét az IT üzemeltető közreműködésével az információbiztonsági felelős jogosult előzetesen ellenőrizni, s a 11. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás fejezetben meghatározottak szerint a Jegyző engedélyezi.

IT üzemeltető feladata:

Szoftver megfelelőség ellenőrzésében közreműködés.

30.9 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

A Hivatal név/cím feloldási szolgáltatást külső, informatikai, illetve telekommunikációs szolgáltató partnertől vesz igénybe. A szolgáltatás igénybe vételének feltétele, hogy a szolgáltató biztosítson elsődleges és másodlagos (tartalék) kiszolgálót. A Hivatal által használt EIR-ekhez hozzáférést biztosító munkaállomásokon, kiszolgálókon, illetve hálózati eszközökön a szolgáltatás igénybevételéhez szükséges beállítások dokumentált elvégzése a 23.6 Konfigurációs beállítások fejezet előírásainak alkalmazásával az IT üzemeltető feladata.

IT üzemeltető feladata:

Menedzselhető hálózati eszközök konfigurálása.