MAXENTROP KFT

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata

Informatika Biztonsági Szabályzat kiegészítése az ASP rendszerek informatikai biztonsági követelményekről

Kelt: 2021.10.01. Hatálybahelyezte Informatikai biztonsági célok, követelmények

Készítette: Maxentrop Kft.

Általános rész

Cél, a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata által kezelt adatok biztonságának a megteremtése. Továbbá az információbiztonsági követelményeknek való megfelelés biztosítása. E szabályzat kiegészítésnek összhangban van az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel, a hozzátartozó 41/2015. (VII. 15.) BM rendelettel, valamint a 257/2016. (VIII. 31.) Korm. rendelettel.

További cél, hogy a szabályzat egységes szerkezetbe foglalja a Hivatal által működtetett ASP rendszer és annak a felhasználóival szemben támasztott informatikai biztonsági követelményeket.

Az önkormányzati ASP rendszer kapcsán kiemelten kezeljük a(z) Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata (továbbiakban Hivatal) kapcsolatos biztonsági kockázatokat. Mivel a Hivatal a saját infrastruktúráját fogja használni az ASP rendszer és alkalmazások igénybe vétele során, így a felhasználói rendszerek biztonsága nagymértékben befolyásolja a teljes önkormányzati ASP rendszer biztonságát.

A Hivatal vezetőjének célja és feladata, hogy minimalizálja a kliens (felhasználó) oldali kockázatokat.

Ennek következtében, szükséges meghatározni ASP-ben a jogosítások kérdését, és a fluktuáció miatt a felhasználók jogosításának időszakos, Hivatal szintű ellenőrzését és esetleges korrekcióját.

Általános biztonsági követelmények

- Az ASP Központtól kapott szoftveres tanúsítvány és annak jelszava nem adható át az ASP Központ által nem feljogosított személynek.
- Az önkormányzati ASP rendszerben csak a „257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről” jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bárminemű fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.
- Az önkormányzati ASP rendszerben tesztelést végezni csak az idézett Korm. rendeletben meghatározott felek jogosultak.
- Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb.
- A tenant adminisztrátor (jogosultságokat kiosztó vezető) törekszik a legkisebb jogosultság kiosztásához a felhasználók körében. A jogosultságok kiosztásánál figyelembe veszi a szervezeti és működési szabályzatot, amely nem kerülhet ellentmondásba a Hivatal IBSZ-szel. Az ASP Központ egy esetleges biztonsági

incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben szerepeltetjük. Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

- A Jegyző az önkormányzati ASP-t ért biztonsági incidensek észlelését jelenti az ASP Központ (és az informatika biztonsági felelős) felé is a Kormányzati Eseménykezelő Központ mellett. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg. Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi. A Hivatal vezetőjének további kötelezettségei is vannak biztonsági incidensek kapcsán (pl. Kormányzati Eseménykezelő Központtal történő kapcsolatfelvétel), melyet a jogszabályok részleteznek.
- Ha az önkormányzati ASP-t üzemeltetői, működtetői oldalon éri biztonsági incidens, az ASP Központnak kötelessége értesítést elhelyeznie a Tájékoztatási Portál nyilvánosság elöl elzárt felületén, megjelenítve a lehetséges elhárítási határidőt, illetve a keretrendszer elérhetősége esetén, a keretrendszer felületén is megjeleníteni ezeket az információkat. Ebben az esetben az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.
- A Korm. rendelet szerinti üzemeltető és működtető felek a Hatóság kérésére, utasítására is leállíthatják az önkormányzati ASP rendszert, vagy annak bizonyos elemeit (pl. kibertámadás esetén). Ebben az esetben az ASP Központ tájékoztatása addig nem fog megtörténni, amíg az incidens kiváltója, okozója, felderítése akadályokba ütközhet, azaz a Hatóság írásbeli engedélyezéséig.
- A szerződésben meghatározott tenant adminisztrátorok rendszerbe történő „felvitelét” az ASP Központ végzi el az önkormányzat által megküldött adatlap alapján.
- A privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot osztanak. Ezt a tevékenységet az önkormányzati jegyző felelősségi és hatásköre.
- Egy önkormányzati fióknál (tenantnál) minimum egy felhasználó karbantartónak szükséges „lenni”, ezt a rendszer figyeli (pl.: nem lehet zárolni, vagy elvenni tőle a jogot, ha csak egyedüli felhasználó karbantartó a tenantnál).
- A rendszer használata során elvárt, hogy a privilegizált joggal rendelkező munkatársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használják.
- A privilegizált joghoz tartozó bejelentkezési azonosítót zárt borítékban, biztonságosan zárható helyen tároljuk.

A tenant adminisztrátor feladatai:

- új felhasználók (userek) rögzítése,
- meglévő felhasználók adatainak módosítása,
- felhasználók zárolása (szükség szerint),
- felhasználói jogosultságok (szerepkörök) kiosztása,
- felhasználói jogosultságok módosítása, megvonása,
- helyettesítések beállítása, eltávolítása,
- felhasználói csoportok létrehozása, módosítása, törlése (ugyanazon szerepkörök kiosztása több felhasználónak),
- üzleti napló megtekintése (a rendszerben történő változásokat lehet lekérdezni, követni).

Jogszabályi hivatkozások

- Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.
- 257/2016. (VIII. 31.) Korm. rendelet

Az IBSZ kiegészítés területi hatálya

A szabályzat tárgyi hatálya kiterjed a Hivatal ASP-vel kapcsolatos tevékenysége során keletkezett, kezelt, feldolgozott, tárolt adatokra és információkra, a számítástechnikai eszközökre, dokumentációikra, és az azokat körülvevő környezetre, valamint a szoftverekre, adatbázisokra, a kapcsolódó dokumentációkra és az adatbiztonsági nyilvántartásokra.

A szabályzat személyi hatálya kiterjed a Hivatal ASP rendszerrel jogosultan kapcsolatba kerülő köztisztviselőire, ügykezelőire, munkavállalóira, illetve egyéb munkavégzésre irányuló, egyéb jogviszonyban álló személyekre, továbbá a választott képviselőkre és a Hivatallal szerződéses kapcsolatban álló vállalkozóira és azok alkalmazottaira. E dokumentum a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat mellékletét képezi.

Az ASP rendszerek fizikai működésének területei:

Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata

Székhely: Tolna megye 7150 Bonyhád, Széchenyi tér 12.

Védelmi intézkedések

A védelmi intézkedések megvalósulásának jelentős részét az ASP Központ biztosítja. Tekintettel azonban arra, hogy az adatkezelés a Hivatal helyszínein, a Hivatal munkavállalói és szerződött partnerei által is megvalósul, így biztonsági elvárások egy része a Hivatal hatáskörébe tartozik.

Az informatikai rendszerek ASP általi besorolása a Hivatal Informatikabiztonsági szabályzatában lett dokumentálva. Jelen szabályzat csak az ASP 2-es szintnél magasabb (a MÁK által meghatározott) védelmi kötelezettségeket, elvárásokat taglalja. A 2-es szintnek való megfelelést a Hivatal hatályos Informatikabiztonsági szabályzata írja le.

Adminisztratív védelmi intézkedések

Az informatikai környezet fő komponensei:

- Munkaállomások beüzemelés
- Nyomtatók üzembe állítása
- Hálózati aktív eszközök beüzemelése, hálózat kiépítése
- Vírusvédelmi rendszer beüzemelése
- Tűzfal beüzemelése
- Internetkapcsolat üzembe állítása

Az infrastruktúra felállításának főbb feladatai

- Tenant létrehozása a Keretrendszerben (ASP. KERET), Tenant adminisztrátor felvétele a Keretrendszerben (ASP.KERET).
- Adatbázisok létrehozása a Gazdálkodási (ASP. GAZD) és szakrendszerben.
- Tenant felhasználók felvétele és szerepkörök összerendelése a Keretrendszerben (ASP. KERET).
- Tanúsítványok elkészítése és hozzárendelése.
- Tanúsítványok kiosztása önkormányzati felhasználók között.

Feladatok az IT biztonsági feltételek megteremtésére, mind a 2-es biztonsági szint mind az ASP működtetéséhez elvárt szinteknek való megfelelésben.

- Önkormányzati biztonsági szintjének meghatározása.
- A meghatározott biztonsági szinthez kapcsolódó védelmi intézkedések biztosítása.
- Információbiztonsági szabályozások kialakítása, szükség szerinti módosítása, jóváhagyása, kihirdetése.
- Biztonsági auditra való felkészülés.

Fontos, hogy:

- egy az ASP-vel kapcsolatos audit tevékenység csak a Hatóság írásbeli engedélyével végezhető el. Erről az önkormányzatnak tájékoztatja a Magyar Államkincstárt.
- az ASP rendszeren külsős Fél, vagy szervezet nem végezhet sérülékenységi vizsgálatot a Hatóság írásbeli engedélye nélkül. Ezen vizsgálati tényről az önkormányzat tájékoztatja a Magyar Államkincstárt.

Munkaállomásra vonatkozó biztonsági elvárások

Az ASP rendszerhez csatlakozó eszközök karbantartásáról, változáskövetéséről a következők figyelembevételével gondoskodunk:

- A folyamatot változáskövetési eljárásrendbe rögzítjük.
- A munkaállomásokon telepítve van vírusvédelmi program, a legfrissebb vírus definíciós adatállománnyal. A végpontvédelem tartalmazzon e-mail (csatolmány) védelmet is.
- A munkaállomáson megoldott a böngésző megfelelő biztonsági beállítása.
- A tervszerű beavatkozásokhoz karbantartási időablak jelölünk ki.
- A munkaállomások programfrissítése, különös tekintettel a legfrissebben kiadott security patch komponensekre felügyelt.
- A telepítő programok, a licensz azonosítók zárható helyen vannak tárolva.

A munkaállomások elhelyezésénél gondot fordítunk, hogy:

- a készülékek olyan módon legyenek a hivatalban elhelyezve, hogy azokat az ügyfelek ne tudják elérni,
- a monitor kijelzési képét az ügyfelek ne tudják elolvasni,
- ideiglenesen magára hagyott készülékek zárolása, képernyővédő aktiválása megoldott legyen,
- munkaidő végén a munkaállomások kikapcsolása történjen meg.

Az ASP központhoz csatlakoztatott infrastruktúra elemeknél megoldjuk a:

- a naplóinformációnak a védelmét,
- hiba esetén a naplóbejegyzések elemzését,
- a rendszer hozzáférés ellenőrzését.

A vírusvédelmi eljárások követelményei

- Meghatározzuk a vírusfertőzés megelőzésére vonatkozó szabályokat. (pl. működő vírusvédelmi rendszer nélkül munkaállomást, laptopot, számítógépes hálózatot nem szabad üzemeltetni. Továbbá a vírusvédelmi program vírus definíciós állományit a legfrissebb állapotban tartja.)
- A teendőket rögzítjük egy vírusfertőzés esetén.
- Vírustámadás esetén szükség szerint a vírusriadót elrendeljük.
- Sérülés, vírusfertőzés után az elvárt helyreállítási eljárások meghatározzuk.

Hálózat védelme

Az informatikai biztonságra és hálózati elérésre vonatkozó minimális és ajánlott feltételek megfogalmazása során az internet eléréshez és a hálózat kiépítéséhez, bővítéséhez szükséges eszközöket meghatároztuk (pl. router, switch, tűzfal.)
A rendszer üzemeltetésével kapcsolatos elvárások:

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) megváltoztatjuk. Az azonosítók zárt borítékban, és biztonságosan zárható helyen tároljuk. Csak előre kijelölt, privilegizált felhasználóknak engedélyezzük bejelentkezni a kérdéses eszközökbe.
- A hálózati végpontokat védjük. A lehetőségek figyelembevétele mellett pl. port security, esetleg 802.1x szabványnak megfelelően.
- Az eszközök hálózatba történő illesztéséről dokumentáció készül.

- Az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történik.
- A menedzselhető eszközök legfrissebb konfigurációja elmentve és zárható helyen tároljuk.

Informatikai határvédelem, tűzfal

- A szervezet internethez való csatlakoztatása csak a központi tűzfalon keresztül történhet meg.
- A tűzfal szabályokat dokumentáljuk és azok zárható helyen, tároljuk.

A tűzfal szabályok módosítása a kijelölt felelős előzetes, írásbeli engedélye alapján történhessen meg.

Mobil eszközök használata

Az informatikai biztonság megfelelő megteremtés és szinten tartása miatt külön gondoskodunk a mobil eszközök használatainak a szabályozásáról. Ehhez a betartandó szempontok a következők:

- A mobil eszközök használatát minden esetben előzetes jegyzői engedélyezés előzni meg.
- A mobil eszközök (pl. notebook) használatára a munkaállomásokra vonatkozó szabályok is érvényesek.
- Kidolgozzuk a mobil informatikai eszközök igénylésének, kiadásának, visszavételének, nyilvántartásának üzemeltetésének a folyamatait.
- Továbbá azokat a szabályokat, amelyek az eszközök hivatalon kívüli kivitelére, az eszközök javítására, esetleges elvesztésére, vagy a selejtezésére vonatkoznak.

1. Szervezeti szintű alapfeladatok

Az alapfeladatokat a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

2. Kockázatelemzés

Az alapfeladatokat a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

3. Rendszer és szolgáltatás beszerzés

Az alapfeladatokat a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

3.1. Erőforrás igény felmérés

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésben működtetett elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházások tervezése részeként;
- elkülönítetten kezeli az ASP-vel kapcsolatban saját működtetésű az elektronikus információs rendszerek biztonságát leíró dokumentumokat a beruházás tervezési dokumentációjában.

3.2. Beszerzések

A Jegyző az ASP-vel kapcsolatban saját működtetésű, az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

- a funkcionális biztonsági követelményeket;
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- a biztonsággal kapcsolatos dokumentációs követelményeket;
- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

3.3. A védelem szempontjainak érvényesítése a beszerzés során

- A Jegyző védi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.
- A Jegyző ugyancsak szerződéseses követelményként határozza meg az ASP-vel kapcsolatban saját működtetésű rendszerrel kapcsolatban a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

4. Üzletmenet (ügymenet) folytonosság tervezése

A Hivatal az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerek rendelkezésre állásának, valamint az EIR-ekben tárolt, illetve kezelt adatok sértetlenségének és rendelkezésre állásának megőrzése érdekében a munkavégzéshez szükséges informatikai erőforrások kiesésére vonatkozóan tervet készít, amely tartalmazza az érintett EIR-eket, az alapfeladatokat és funkciókat, a problémakezeléshez szükséges azonnali intézkedéseket, valamint a helyreállítási idő függvényében szükséges alternatív (tartalék) intézkedéseket, a

helyreállításhoz szükséges feladatokat és az azokhoz kapcsolódó prioritásokat, az intézkedések végrehajtásáért felelős szerepköröket feladataikat.

A Hivatal az alábbi, megelőző védelmi intézkedéseket teszi:

- megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását; ennek érdekében a mentési adathordozók tárolására elsődleges és szükség szerint másodlagos tárolási helyszínt jelöl ki, továbbá kialakítja a mentési adathordozók biztonságos tárolásának feltételeit (pl.: zárható lemezszekrény vagy páncélszekrény, elektronikus védelemmel ellátott helyiség, stb.);
- gondoskodik az informatikai eszközök rendszeres karbantartásáról, szükség szerinti javításáról;
- a kieső informatikai erőforrások (pl.: hardvereszközök) pótlásáról szükség esetén rendkívüli beszerzéssel gondoskodik;

4.1. Kritikus rendszerelemek meghatározása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekben meghatározza az elektronikus információs rendszerek alapfunkcióit támogató kritikus rendszerelemeket az üzletmenet folytonossági tervben. A tervvel kapcsolatos részleteket a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

4.2. A folyamatos működésre felkészítő képzés

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerek folyamatos működésére, felkészítő képzést tartat az Informatikabiztonsági felelős révén a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő meghatározott (az Informatikabiztonsági vezető ajánlása, de legkésőbb az éves oktatás során) időn belül;
- legalább évente egyszer, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik. Az oktatásról szóló jegyzőkönyvet, a 6.4 pont szerinti dokumentált formában megőrzi.

4.3. Üzletmenet folytonosság elérhetőség

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszer biztonsági tárolási helyszínéhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére – a Jegyző, vészhelyzeti eljárásokat dolgoz ki az üzletmenet folytonossági tervben.

4.4. Infokommunikációs szolgáltatások

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereit (a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével) amennyiben jogszabályi kötelezettsége van a saját működtetésű rendszerének folyamatos fenntartására, tartalék infokommunikációs szolgáltatásokkal létesíti és üzemelteti. Erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

4.5 Szolgáltatás-prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, akkor a Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekkel kapcsolatos üzemeltetőktől megköveteli, hogy az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

5. Emberi tényezőket figyelembe vevő - személy – biztonság

Humán erőforrás az ASP-ben

Az ASP rendszereket használó önkormányzati hivatal szervezeti egység vezetőjének a felelőssége, hogy meghatározza az egyes, ASP szakrendszer munkakörökhöz tartozó felelősségeket és feladatokat.

Alkalmasság vizsgálattal kapcsolatos elvárások:

- Az önkormányzati hivatal humánpolitikai szervezet vezetőjének a felelőssége, hogy foglalkoztatás előtt a betöltendő ASP rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelőségi vizsgálatot végezzen el a foglalkoztatni kívánt munkatárs vonatkozásában.
- A kockázattal arányos mértékben mérlegeljük a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség stb.).
- Meggyőződünk arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.
- Az informatikai biztonsági szakterület vezetőjének felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.
- A humánpolitikai szakterület vezetőjének a felelőssége, hogy a foglalkoztatás alkalmával az önkormányzati hivatal munkaköri leírásban rögzítse a kockázatokkal arányosan a titoktartás követelményeit (ASP titoktartási nyilatkozat) és a foglalkoztatás egyéb kikötéseit.

- Az önkormányzati hivatal jogi szakterület vezetőjének felelőssége, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

5.1. Munkakörök, feladatok biztonsági szempontú besorolása

A Jegyző:

- minden az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerrel kapcsolatos és érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot, biztonsági szempontból besorol. A besorolás alapja kétszintű: Jogosultságot adó (tenant adminisztrátor) és végrehajtó (user);
- szükség szerint felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat (ha vannak);
- rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

5.2. A személyek ellenőrzése

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy az (5.1. pont) pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e;
- az (5.1. pont) szerinti munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében szükség szerint kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést (ha szükséges);
- folyamatosan ellenőrzi (az évenkénti felülvizsgálatok alkalmával) e pont szerinti feltételek fennállását.

5.3. Az áthelyezések, átirányítások és kirendelések kezelése

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereknél szükség esetén elvégzi az 5.2. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást;
- logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerekhez;
- szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését;
- a jogviszony változásáról szóban és szükség szerint írásban (pl.: e-mail) értesíti az ASP rendszereket használó szerepköröket betöltő, feladatokat ellátó személyeket.

5.4. A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Jegyző:

- az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
- szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg a Jegyző és a vonatkozó rendeletek által meghatározott személybiztonsági követelményeknek;
- a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;
- előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön írásos (pl. e-mail) értesítést a Jegyzőnek;
- folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

5.5. Belső egyeztetés

A Jegyző a rendszeres Hivatali és Hivatalok közti kommunikációban egyezteti az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszert biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

6. Tudatosság és képzés

A Hivatal minden, munkaköri feladatai ellátása során az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél felhasználására kötelezett munkavállalója számára biztosítja feladatainak és szerepkörének megfelelő mértékben az adott EIR felhasználására, annak biztonsági követelményeire vonatkozóan rendelkezésre álló információkat, dokumentációkat, továbbá az ezzel kapcsolatban esetlegesen elérhető (pl.: központi üzemeltető által biztosított) képzésen történő részvételt.

A fentiek a Hivatal által használt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél illetve a Hivatal által kezelt adatokhoz hozzáféréssel rendelkező, a Hivatallal egyéb munkavégzésre irányuló jogviszonyban álló személyekre és szervezetekre is vonatkozik, de ezen képzések nem a Hivatal feladata. Azt előírja a fenti személyeknek, szervezeteknek, oly módon, hogy igazolják annak teljesítését.

Az egyéb információbiztonsági tárgyú képzéseken, biztonságtudatosító programokon, oktatásokon történő részvétel igazolása az adott képzés, oktatás jellegétől és lebonyolítási módjától függően történhet a képzést, oktatást szervező szervezet – amennyiben az nem a Hivatal – által kiadott igazolás, illetve jelenléti ív formájában.

6.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel.

A Jegyző az IB szakmai kapcsolattatását az IB felelősön keresztül valósítja meg.

6.2. Belső fenyegetés

A Jegyző a biztonságtudatossági képzések keretében, végezteti az érintett személyeknek a belső fenyegetések felismerésére való felkészítését, hogy tudatosítsa jelentési kötelezettségüket. A képzésben és tudatosításban hangsúlyt fektetünk arra, hogy a hibákat, incidenseket ne titkolják el, hanem jelentsék a Jegyzőnek.

6.3. Szerepkör, vagy feladat alapú biztonsági képzés

A Jegyző szerepkör, vagy feladat alapú biztonsági képzést nyújtat az Informatikabiztonsági felelős által az egyes szerepkörök szerinti, felelős személyeknek:

- az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi és évenkénti rendszerességgel.

6.4. A biztonsági képzésre vonatkozó dokumentációk

A Jegyző:

- dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;
- a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi. A dokumentumot az iratkezelési szabályzat előírásai szerint őrizzük meg és tároljuk.

Fizikai védelmi intézkedések

7. Fizikai védelmi eljárásrend

Fizikai biztonság megteremtése ASP-ben

A fizikai biztonság meghatározásánál az ASP-t futtató objektum tekintetében, az önkormányzati hivatal biztonsági zónákat jelölni ki, melyet minden esetben az önkormányzati hivatali szervezete határoz meg, saját eljárásrendjében, az alábbiak figyelembevételével:

- Az épület földrajzi elhelyezkedését. Lehetőleg a bejutás ellenőrzött legyen.
- Az épület építészeti, épületgépészeti adottságait figyelembe vesszük.
- Ügyfélforgalom mértékét,
- az ASP felhasználóknak nyújtott szolgáltatásokat és az
- információk osztályozása, minősítését figyelembe vesszük.

Őrzés, védelem szempontjai

- A törekszünk az élő erős őrzés megvalósítására. Ha ez megvalósul, akkor szabályzatban rögzítjük az őrszolgálat működési rendjét, az incidenskezelés folyamatát.
- Az önkormányzati hivatalok ASP-t is futtató helységeibe a bejutás ellenőrzötten történik az oda beosztottakon és ügyintézés miatt jelenlévőkön kívül (pl. vendégek, karbantartók stb.) ellenőrzésről nyilvántartást vezetünk.
- Hivatalunk a lehetőségeihez képest kialakít az objektum védelme érdekében behatolás védelmi, tűzjelző és szükség szerint video-megfigyelő rendszert. A biztonsági rendszerek adatai archiváljuk, és akár több hónapra visszamenőleg megőrizve a hazai jogszabályokat figyelembe véve.
- Földszinti ablakokon lehetőség szerint vasrácsokkal védekezünk az illetéktelen behatolástól. Az informatikai biztonsági felelős rendszeresen (évente) ellenőrzést hajt végre, az eredményt jegyzőkönyvbe rögzíti, mely része, kiegészítése a cselekvési tervnek. A jegyzőkönyvet az ASP Szolgáltatási szerződésben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre adja át.

7.1. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

A Jegyző engedélyhez köti és ellenőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerei adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

7.2. A kimeneti eszközök hozzáférés ellenőrzése

A Jegyző jogosultsághoz köti és ellenőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereihez, kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá. A jogosultság történhet szóban, szerződés és munkaköri feladat keretében.

7.3. A fizikai hozzáférések felügyelete

A Jegyző jogosultsághoz köti és ellenőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és szükség esetén reagáljon arra.

7.4. Behatolás riasztás, felügyeleti berendezések

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél (ha azt naplózást biztosító védelmi rendszer biztosítja) rendszeresen átvizsgáltatja a fizikai hozzáférésekről készült naplókat.

7.5. A látogatók ellenőrzése

A Jegyző az érvényes tv.-ben meghatározott ideig megőrzi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél helyt adó létesítményekbe történt látogatói belépésekről szóló információkat. Az ilyen helyiségekbe való belépés dokumentálását, (Hivatali terület) amennyiben nincs elektronikus védelmi rendszer, akkor papíralapon dokumentáljuk és őrizzük meg.

7.6. Áramellátó berendezések és kábelezés

A Jegyző a szükséges mértékben és optimális módon védi az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereit árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben (kábelcsatornák, rejtett kábelezés). Az erőforrásokat koncentráltan tartalmazó helyiségekben a hőmérsékletnek és a páratartalomnak az erőforrások biztonságos működéséhez szükséges szinten tartása és folyamatos figyelemmel kísérése, ellenőrzése céljából erre alkalmas légkondicionáló berendezést üzemeltet.

7.7. Tűzvédelem

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerei számára amennyiben azt arra alkalmas, elkülönített helységben működteti, független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő és a vonatkozó rendeleteknek megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

7.8. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél megköveteli, hogy az elektronikus információs rendszer optimális és célszerű kialakítással védjék a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek legyenek.

7.9. Be- és kiszállítás

A Jegyző mindig egyedileg engedélyezi, vagy tiltja, továbbá figyelteti és ellenőrzi a létesítménybe bevitt, onnan kivitt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeket, és nyilvántartást vezettet ezekről. A be- és kiszállítás felügyeletét, figyelemmel kísérését a Hivatallal munkavégzésre irányuló szerződéses jogviszonyban álló személy felügyeletével megbízott munkatárs esetében is

engedélyhez köti, szakmai ellenőrzésében szükség szerint közreműködik az IT üzemeltető, rendszergazda.

7.10. Az elektronikus információs rendszer elemeinek elhelyezése

A Jegyző úgy helyezi, vagy helyezteti el az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

7.11. Karbantartók

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemei karbantartását kizárólag a Hivatallal e feladat ellátására vonatkozóan szerződéses jogviszonyban álló szervezetek, illetve személyek az IBSz és mellékleteiben meghatározottak szerint, s minden esetben csak felügyelet mellett végezhetik. A jegyző továbbá:

- fenntart egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- felhatalmazást ad a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

7.12. Időben történő javítás

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeihez, karbantartási támogatást biztosít, szerződést köt az időben történő javítások megelőző karbantartások elvégzésére.

Logikai védelmi intézkedések

8. Általános védelmi intézkedések

8.1. Az elektronikus információs rendszer kapcsolódásai

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett rendszerek esetében a kapcsolódás szabályait, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát a rendszer tulajdonosa, működtetője határozza meg és dokumentálja. Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek használatba

vétele esetén a Hivatal gondoskodik arról, hogy ugyanezen információk a rendszer dokumentációiban szerepeljenek.

A Jegyző feladata gondoskodni arról, hogy az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereivel kapcsolatba kerülő munkatársai, valamint a Hivatallal munkavégzésre irányuló egyéb szerződéses jogviszonyban lévő személyek a feladatellátásukhoz szükséges mértékben a rendelkezésre álló rendszer-, illetve felhasználói dokumentációkat megismerjék.

8.2. Belső rendszer kapcsolatok

A Jegyző általa kiadott, engedélyhez köti az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek összekapcsolását.

8.3. Külső kapcsolódásokra vonatkozó korlátozások

A Hivatal által használt az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek, illetve rendszerelemeik külső elektronikus információs rendszerhez történő kapcsolódása kizárólag a Hivatal által igénybe vett vagy jóváhagyott hálózati kommunikációs csatornán (internet kapcsolat, adathálózat) keresztül a Jegyző jóváhagyásával engedélyezett.

A végrehajtható programok, script-ek (pl.: Java Applet, JavaScript, VB Script, CGI, stb.) letöltését, futtatásának lehetőségét, valamint web és alkalmazásba csomagolt ActiveX objektumok működését letiltjuk az internet böngésző programokban, továbbá gondoskodunk arról, hogy a böngésző alkalmazás biztonsági frissítése rendszeresen megtörténjen.

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett rendszerek esetében a kapcsolódás biztonsági követelményeit – fentieknél esetenként szigorúbb korlátozását, illetve az attól való eltérést – a rendszer működtetője határozza meg, a Hivatal gondoskodik annak alkalmazásáról, szabályok betartásáról.

9. Tervezés

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek tervezéssel kapcsolatos vonatkozó részleteket a Bonyhádi Közös Önkormányzati Hivatal és Bonyhád Város Önkormányzata Informatikai Biztonsági Szabályzat tartalmazza.

10. Konfigurációkezelés

10.1. Legszűkebb funkcionalitás

A Hivatal az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek a felügyeletét és 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. Továbbá meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

10.2. Duplikálás elleni védelem

A Jegyző ellenőrzi, hogy az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

11. Karbantartás

11.1. Adathordozó ellenőrzés

A Jegyző ellenőrizteti a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

11.2. Távoli karbantartás

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;
- csak akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;
- hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;
- nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;
- kötelezi a felhasználókat, hogy lezárják, a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

12. Adathordozók védelme

12.1. Adathordozók tárolása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- fizikailag egyedileg azonosítja, ellenőrzi és biztonságosan tárolja az adathordozókat az arra engedélyezett vagy kijelölt (elzárt) helyen;
- védi (és ezt a munkatársaitól is megköveteli) az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

A hivatali munkavégzéshez a Hivatal által biztosított, beépített adathordozót tartalmazó mobil eszközök (pl.: laptop, tablet, okostelefon) és mobil adattároló eszközök (pl.: memóriakártya, külső háttértároló eszköz vagy merevlemez, optikai adathordozó lemez, stb.) fizikai védelméről és biztonságos tárolásáról és kezeléséről a használatára jogosult személy, munkavállaló köteles gondoskodni. Használaton kívül az eszközt, adattárolót elzárjuk, illetve illetéktelenek számára hozzáférhető helyen folyamatos felügyelet nélkül, őrizetlenül hagyni (pl.: közterületen parkoló zárt gépjárműben is) nem szabad!

12.2. Adathordozók szállítása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél :

- az IBSZ-ben leírt biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;
- biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;
- feljegyzésben dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;
- korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

12.3. Kriptográfiai védelem

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél megköveteli, hogy kriptográfiai mechanizmusokat alkalmazzanak a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás, használat folyamán (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.). A kriptográfiai védelem megvalósítása az eszköz e célt szolgáló funkciójának használatával történhet (pl.: BitLocker meghajtótitkosítás, VPN), melyek esetében a technológia (pl.: OpenVPN, SSTP, stb.), illetve az általa alkalmazott rejtjelezési algoritmus (pl.: AES) megfelelősége nemzetközileg elismert információbiztonsági szabvány alapján (pl.: CC, FIPS) igazolt.

12.4. Ismeretlen tulajdonos

A Jegyző megtiltja az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

13. Azonosítás és hitelesítés

ASP rendszerbe történő belépés, authentikáció

Az ASP eSZIG-gel történő azonosítás során személyes adathoz az ASP rendszer nem fér hozzá. Belépéskor ugyanis az e-személyi érvényességét közvetlenül a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalának (a továbbiakban: KEKKH) szervere ellenőrzi. A KEKKH szervere az ASP rendszernek egy ún. hash-kódot (RID) ad vissza, mely azonos okmány esetén mindig ugyanaz, de ez a kód nem fejthető vissza személyes adattá. Az ASP rendszer ehhez az anonim hash-kódhoz rendeli a felhasználót.
Az elektronikus személyigazolvánnyal történő authentikáció során a következő szabályzókra megkülönböztetett módon figyelünk:

- Minden ASP rendszert használó munkatársnak rendelkezik eSZIG-el.
- Az eSZIG használatához szükséges a kártyaolvasó számítógépre történő telepítése.
- Az ASP rendszerbe történő sikeres beléptetés érdekében a Keretrendszerbe rögzített felhasználói fiók és az eSZIG összerendelése szükséges.
- A személyi igazolvány kártyát csak a tulajdonosa használhatja, azt ASP rendszer authentikációs folyamat céljából másnak átadni tilos.
- Az hivatal vezetője a Jegyző gondoskodik arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen.

13.1. Jelszó (tudás) alapú hitelesítés

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja;

A jelszavas hitelesítést alkalmazó rendszerelemeken kötelező a jelszavas védelem beállítása és alkalmazása.

A felhasználói jelszavakra vonatkozó a mindig a technikailag elvárt, de minimálisan alkalmazandó általános jelszó követelmények:

- a jelszó minimális hossza (legrövidebb jelszó): 8 karakter;
- a jelszó bonyolultsága (komplexitás): tartalmaz legalább egy kis- és nagybetűs, speciális karaktert, valamint számjegyet;
- előző jelszavak megőrzése: legutolsó 5 jelszó tárolása;
- a jelszavak minimális és maximális élettartama: 0 és 90 nap.

A meghatározott jelszóképzési szabálytól eltérni a jelszó hosszát, bonyolultságát illetően a magasabb védelmi szintet jelentő irányba, felfelé lehet (pl.: „jelszó helyett jelmondat”-elv alkalmazásával).

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Hivatal a rendszer tulajdonosa által meghatározott jelszóképzési szabályokat alkalmazza.

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 a Jegyző gondoskodik azok biztonságos megőrzéséről és kezeléséről (lezárt borítékban, páncélszekrényben).

A felhasználói azonosítók és jelszavak elektronikus tárolása, nyilvántartása kizárólag önálló és biztonságos hitelesítési megoldással rendelkező vagy egyéb kriptográfiai védelemmel ellátott módon, offline tárolással engedélyezett; nyílt formában vagy mobil infokommunikációs eszközön valamint online jelszótároló rendszerben tilos!

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 kikapcsoljuk!

13.2. Birtoklás alapú hitelesítés

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- hardver token alapú hitelesítése esetén, olyan mechanizmusokat alkalmaz, amely megfelel a Jegyző által meghatározott minőségi követelményeknek, vagy
- az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal.

Ha a Hivatal hatáskörébe tartozik, akkor azt minden esetben átadás-átvételi bizonylattal dokumentálja. Az átadás-átvétel dokumentumainak megőrzéséről a Hivatal a hatályos iratkezelési szabályainak megfelelően gondoskodik.

A jegyző a birtoklásalapú hitelesítésre szolgáló eszközök használati idejét, továbbá ismételt felhasználhatóságának feltételeit az érintett EIR igénybevételére vonatkozó szabályok, valamint a kibocsátó, illetve a gyártó ajánlásainak megfelelően alakítja ki, illetve alkalmazza.

13.3. Személyes vagy megbízható harmadik fél általi regisztráció

A Jegyző meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le a Jegyző által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

14. Hozzáférés ellenőrzése

14.1. A felelősségek szétválasztása

A Jegyzőaz az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- szétválasztja az egyéni felelősségeket;
- dokumentálja az egyéni felelősségek szétválasztását;
- meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

14.2. Legkisebb jogosultság elve

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

14.3. Jogosult hozzáférés a biztonsági funkciókhoz

A Jegyző hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

14.4. Nem privilegizált hozzáférés a biztonsági funkciókhoz

A Jegyző kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

14.5. Privilegizált fiókok

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

14.6. A munkaszakasz zárolása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- kötelezi a felhasználókat, hogy 5 perc inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;
- megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

14.7. Képernyőtakarás

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - eltakarjuk.

14.8. A munkaszakasz lezárása

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél automatikusan lezárja a munkaszakaszt a meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

14.9. Vezeték nélküli hozzáférés

A Hivatal épületeiben vezeték nélküli hálózatához hozzáférést a Jegyző engedélyével lehet csak létesíteni, illetve igénybe venni. Kivételt képez ez alól – amennyiben az adott telephelyen elérhető – a Hivatal által biztosított, a Hivatal hálózatáról leválasztott, szeparált nyilvános hálózati hozzáférés (pl.: „vendég" wifi), amelyhez a Hivatal munkatársai is csatlakoztathatják saját mobil eszközeiket.

Hivatali munkavégzés céljára biztosított vezeték nélküli hálózat hozzáférés védelemmel (minimum jelszavas védelemmel) ellátottan és a csatlakoztatható eszközök – például fizikai hálózati címének (MAC address filter) – szűrésével létesíthető.

A Jegyző:

- az engedélyezési és jogosultsági szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
- engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

14.10. Mobil eszközök hozzáférés ellenőrzése

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- az engedélyezési és jogosultsági szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;
- engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

14.11. Titkosítás

A Jegyző teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk

bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

14.12. Korlátozott használat

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

- előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy
- jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

14.13. Hordozható adattároló eszközök

A Jegyző egyedileg korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a jogosultsággal rendelkező személyek számára.

14.14. Információ megosztás

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- elősegíti az információ-megosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információ-megosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;
- automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információ-megosztási vagy együttműködési döntések meghozatalában.

15. Rendszer és információ sértetlenség

15.1. Automatikus frissítés

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

15.2. Biztonsági riasztások és tájékoztatások

A Jegyző az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- folyamatosan figyeli, illetve az informatikai biztonsági felelősön keresztül figyelteti a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri, illetve az informatikai biztonsági felelősön keresztül figyelteti a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
- szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;
- a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
- kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart illetve az informatikai biztonsági felelősön keresztül tartat az érintett, külön jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz, vagy intézkedik annak tételére a megbízott személyekkel, szervezetekkel.

15.3. Bemeneti információ ellenőrzés

Az ASP-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél ellenőrzi a meghatározott információ belépési pontok érvényességét.

Jelen kiegészítés a Hivatali IBSZ-szel együtt értelmezendő, a továbbiakban egy dokumentumként kezelendő. Hatályba lépésének napja megegyezik a Hivatali IBSZ hatálybalépésének idejével.

Bonyhád, 2021. ……..

jegyző

Szerzői jogok

A Hivatal kliens oldali biztonsága megteremtésének táblázatos összefoglalója

Az ASP kapcsán kiemelten kezeljük a Hivatallal kapcsolatos biztonsági kockázatokat. A Hivatal a saját infrastruktúráját fogja használni az alkalmazások igénybevétele során, így a kliens rendszerek biztonsága nagymértékben befolyásolja a teljes ASP rendszer biztonságát.
A lehetséges fenyegetettségek, sebezhetőségek, valamint ezek megelőzésére alkalmazható intézkedések a Hivatalunkban az alábbiak:

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
ASP rendszer önkormányzati, végponti állomásai	Érzékeny adatok ellopása, adatfájlok törlése, ellopása, módosítása.	Hozzáférés védelem beállítása.
	Rosszindulatú program (vírus, trójai faló, stb.) bejuttatása a rendszerbe.	Vírusvédelmi rendszer alkalmazása.
	Vírus, trójai faló, féreg aktiválódása, pl. e-mail csatolmány megnyitásakor.	Vírusvédelmi rendszer alkalmazása.
	Végrehajtható programok, script-ek (Java Applet, JavaScript, VB Script, CGI, stb.) letöltése, pl. az állomás DoS támadásra való felhasználására a felhasználó tudtán kívül.	Böngésző biztonsági beállítása.
	Web és alkalmazásba csomagolt ActiveX objektumok, amelyek a programozó szándékától függően a legkülönbözőbb károkat (gépleállítás, konfiguráció feltérképezés, monitor/billentyűzet elvétel, stb.) okozhatják.	Böngésző biztonsági beállítása.
	Ismeretlen forrásból érkező e-mail-ek és azok csatolmányainak megnyitása.	Vírusvédelmi rendszer alkalmazása, felhasználó oktatása.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	Az Internet böngészőkben meglévő biztonsági „lyukak” megszüntetésére szolgáló javító programok letöltésének elmulasztása. A biztonsági „lyukak” kihasználásával elérhetők a végponti felhasználó érzékeny adatai (jelszó, az állomás konfigurációja, fájl nevek, fájl struktúra, a meglátogatott weblapok címei, stb.).	Legújabb verziók, frissítések telepítése.
	A munkaállomásra letöltött adatlapok (kérdőív, adatszolgáltató formanyomtatvány, stb.) programhibái. A szolgáltatott adatok rejtjelezés nélküli elküldése.	Csak megbízható forrásból származó program használata.
	Vírusvédelmi program frissítésének elmulasztása.	Rendszeres, automatikus frissítés.
	Az igénybevett szolgáltatás letagadása.	Naplózás.
	A munkaállomás ellopása.	Követelményrendszer szerinti fizikai biztonság kialakítása.
	Mobil eszköz ellopása	Az előírt fizikai védelmi eszközök alkalmazása. Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.
Internet	A felhasználó login adatainak (felhasználói-azonosító, jelszó) lehallgatása, ezek segítségével a felhasználó megszemélyesítése.	Rejtjelezett adatátviteli csatorna használata.
	Érzékeny adatok lehallgatása.	Rejtjelezett adatátviteli csatorna használata.
	Adatok lehallgatás és továbbítása megváltoztatott tartalommal elleni védelme.	Hozzáférés-vezérlés kialakítása. Rejtjelezett adatátviteli csatorna. Egyszer használatos jelszó.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	E-mail-ek, elektronikus dokumentumok eltérítése.	Hozzáférés-vezérlés kialakítása.
Tűzfal	Tűzfal-biztonságpolitika hiánya vagy hiányos volta.	Tűzfal-biztonságpolitika elkészítése, vagy aktualizálása.
	Ad hoc vagy nem a biztonságpolitikának megfelelő biztonsági beállítás, vagy üzemeltetés.	Biztonsági beállítások rendszeres ellenőrzése, naplózás, riasztás.
	Portok letapogatása.	Tűzfal biztonsági beállítása.
	IP cím megszemélyesítés, a támadó a védett hálózaton működő számítógép (pl. szerver) IP címét megszerezve egy belső munkaállomást „szimulálva” a tűzfalon keresztül fér hozzá a szerveren levő adatállományokhoz.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása.
	Visszaélés, forrás útvonalválasztással. A támadó a védett belső hálózat felépítésének ismeretében a saját gépében meghatározott útvonallal és belső IP címmel belső gépet „játszik el” és fér hozzá az útvonal végén levő belső géphez.	Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása. Hálózati végpont IP címhez, MAC címhez kötése.
	Szerver típus specifikus biztonsági lyukak az operációs rendszerben. Az aktuális javító- és szerviz csomagok telepítésének elmulasztása.	Operációs rendszerek biztonsági frissítéseinek folyamatos figyelése, végrehajtása.
	A tűzfal távoli, pl. Interneten keresztül történő adminisztrálása.	Tűzfal adminisztrálása csak védett hálózatból, vagy konzolról.
	Vírusvédelmi programok frissítésének elmulasztása.	Vírusvédelmi rendszer folyamatos frissítése.
	Hiányos biztonsági naplózás. A biztonsági naplók értékelésének elmulasztása vagy rendszertelensége.	Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	Hiányos fizikai biztonság.	Követelményrendszer szerinti fizikai biztonság kialakítása.