ASP Informatikai Biztonsági Szabályzat

a
Tiszacsegei Közös Önkormányzati Hivatal

részére

Tiszacsege

Hatályos 2022. január 1-től

A szabályzat a hivatal számára elfogadva:

Dr. Lajter Zoltán
jegyző

TISZACSEGEI KÖZÖS ÖNKORMÁNYZATI HIVATAL * JEGYZŐ

Tartalom

1. Bevezetés 3
2. Alapfogalmak 3
3. Jogszabályi háttér 5
4. A 41/2015. (VII. 15.) BM rendeletben megfogalmazottak alapján történő rendelkezések 5
5. Az Informatikai Biztonsági Szabályzat célja és hatálya 6
   A szabályzat célja 6
   Személyi hatálya 6
   Tárgyi hatálya 7
6. Szerepkörök, feladatok, felelősségek 7
7. Kapcsolódó eljárásrendek 7
8. Informatikai Biztonsági Szabályzat kialakításához ASP specifikus irányelvek 8
9. Az ASP rendszerhez csatlakozás 8
10. Az infrastruktúra felállítása 8
11. IT biztonsági feltételek megteremtése 8
12. Fizikai biztonság megteremtése ASP-ben 8
13. Őrzés, védelem 9
14. Humán erőforrás az ASP-ben 9
15. Oktatás, képzés az ASP-ben 9
16. ASP jogosultság kezelés 10
17. ASP rendszerbe történő belépés, authentikáció 10
18. Csatlakozó önkormányzatok kliens oldali biztonsága 11
19. Munkaállomásra vonatkozó biztonsági elvárások 14
20. Rosszindulatú kódok elleni védelem 14
21. Hálózatbiztonság, hálózatvédelem 14
    Informatikai határvédelem, tűzfal 15
22. Mobil eszközök használata 15
23. Osztályba sorolás eredménye 15
    Jegyző, a szervezet vezetője 17
    Elektronikus információs rendszer biztonságáért felelős személy 18
    A Tenant adminisztrátor feladatai: 19
    A Tenant felhasználók és vele kapcsolatba kerülő külső beszállítók feladatai: 20

1. Bevezetés

Napjainkra az informatikai és kommunikációs rendszerek rendkívül összetetté váltak, és átszövik egész életünket. Olyan komplexet képeznek, amelyek elemei komoly kihatással vannak az egész hivatal működésére. Egy ilyen, rendkívül összetett és nagyfontosságú terület sok ponton van kitéve a működését fenyegető veszélyeknek.
Bátran állíthatjuk, hogy az Informatikai Rendszer stratégiai fontosságú a hivatal életében. Egy ilyen nagyfontosságú területnek, elengedhetetlen, hogy önálló biztonsági koncepciója, valamint kidolgozott biztonsági, védelmi eljárásai legyenek.
Elmondható, hogy a biztonság fogalma nem csupán a támadások elleni védekezést takarja, hanem általában véve a működőképesség fenntartását. Ezért nem is elégséges egyetlen területre kidolgozni a megelőzés és védekezés szabályait, hanem ezt az összes részterületen meg kell tenni.
Az Informatikai Biztonságtechnikai Szabályzat hivatott betölteni azt a szerepet, hogy összefoglaló alapszabályozási rendszerként meghatározza a védendő részterületeket, az Informatikai Rendszer elemeit, a kockázatok mértékének meghatározásához szükséges irányelveket, a megelőzési és védekezési eljárásokra vonatkozó szabályokat.
Jelen dokumentum ezen célok elérése érdekében, a KÖFOP-1.0.0-VEKOP-15-2016-0008 számú projektben kidolgozott irányelvek szerint készült, alkalmazkodva a környezeti sajátosságokhoz, és helyi szervezet működési sajátosságaihoz.

2. Alapfogalmak

Adat
Jelentés nélküli, de önállóan is értelmezhető logikai egység, amelyek az információk alapjául szolgál.

Adatállomány
Az adatok összefogására, rendezett tárolására szolgáló, azonosító névvel ellátott logikai egység.

Adatátvitel
Adatok szállítása elektronikus rendszerek segítségével.

Adatbiztonság
Jogosulatlan adathozzáférés elleni technikai és szervezési eljárások együttes rendszere.

Adatbiztosítás
Azon szabályozó elvek és ezekre épülő szabályozási utasítások összessége, amelyek célja az adatbiztonság garantálása.

Adatfeldolgozás
Az adatok rendszerezése előre meghatározott rendező elvek alapján, a belőlük származó információk kinyerése céljából.

Adatvédelem
Az adatok kezelésével kapcsolatos törvényi szabályozások összessége.

Bejelentkezés
Az informatikai rendszer megfelelő elemeinek használata előtti rendszer-inicializálások együttes megnevezése, a jogosultságoknak megfelelően.

Bizalmasság
A bizalmasság azt jelenti, hogy a hivatalnál az adatokhoz és a belőlük származó információkhoz csak az arra jogosult munkatársak férhetnek hozzá.

Biztonsági koncepció
A hivatal által kidolgozott biztonsági politika elvi alapjait magába foglaló dokumentum, illetve dokumentum részegység.

Elérhetőség
Az Informatikai Rendszer elemeinek az adatfeldolgozás során szükséges mértékben, helyen és időben történő igénybevételi lehetősége.

Érték
Az informatikai rendszer elemeinek jelentősége, illetve azok hivatalon belül történő használatának, felhasználásának jelentősége anyagi, vagy erkölcsi mértékkel megadva.

Hálózat
Számítógépek kommunikációs csatornákon keresztül történő összeköttetése (az eszköz fizikai formájától függetlenül), melynek célja a számítógépek közötti. adatátvitel biztosítása.

Hitelesítés
Az informatikai rendszer megfelelő elemeinek használata előtt történő azonosítási eljárás, amely lehetővé teszi a feltételek nélküli felismerhetőséget az arra jogosultak számára.

Hozzáférés
Eljárás, amely az informatikai rendszer használója számára elérhetővé teszi a rendszerben adatokként tárolt információkat.

Információ
Önálló jelentéssel bíró adat vagy adathalmaz.

Kockázat
Valamely fenyegető tényezőből eredő fenyegetettség mértéke, melynek összetevői a kár nagysága., és a bekövetkezés lehetséges gyakorisága.

Mentési rendszer

Az adatok rendelkezésre állását lehetővé tévő rendszer, amely a biztonsági másolatok tárolására szolgál.

Működőképesség
Az informatikai rendszernek, mint egésznek, valamint az elemeinek a hivatal számára elvárt, és a hivatal működése szempontjából igényelt üzemelésének fennmaradása.

Rendelkezésre állás
Az informatikai rendszernek, illetve egyes elemeinek az az állapota, amikor annak működőképessége, illetve elérhetősége nincs akadályozva.

Támadás
Valamely személynek vagy szervezetnek azon szándékkal indított akciója, hogy azzal az informatikai rendszert, illetve annak valamely elemét veszélyeztesse, abban károkat okozzon.

Üzenet
Hálózatokon továbbított adatcsomagok, függetlenül azok információs tartalmától.

3. Jogszabályi háttér

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint 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 értelmében az állami és önkormányzati szerveknek rendelkezniük kell Informatikai Biztonsági Szabályzattal.

A szabályzat kialakításánál az említett jogszabályokon túl figyelembe kell venni az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendeletet.

A konkrét jogszabályok elérhetőségei a következők:

- 2013. évi L. törvény
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV
- 41/2015. (VII. 15.) BM rendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500041.BM
- 257/2016. (VIII. 31.) Korm. rendelet
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600257.KOR&timeshift=fffffff4&txtreferer=00000001.TXT

4. A 41/2015. (VII. 15.) BM rendeletben megfogalmazottak alapján történő rendelkezések

Szervezeti szintű alapfeladatok adminisztratív védelmi intézkedés alapján, a rendeletnek megfelelően a Tiszacsegei Közös Önkormányzati Hivatal felelős vezetője (Jegyző) a következőket határozza meg:

- Jelen dokumentum a Tiszacsegei Közös Önkormányzati Hivatal dolgozóira és külső informatikai beszállító partnereire érvényes követelmények szerint dokumentált, a bevezetésre került ASP rendszerhez kapcsolódó Informatikai Biztonságtechnikai Szabályzat (továbbiakban IBISZ).
- A szabályzat a dolgozók és informatikai beszállítók számára történő kihirdetéssel és a jogosultak számára történő közzététellel lép érvénybe, a szabályzatban megfelelő helyeken szereplő napokon.
- Jelen dokumentum tartalma egy évenként felülvizsgálandó és aktualizálandó, az aktuális jogszabályi és technológiai követelményeknek megfelelően, illetve soron kívül abban az esetben, ha ez jogszabályi változás miatt szükséges, illetve jelentős technológiai változás teszi indokolttá.
- Jelen szabályzat megismerésekor az azt megismerő jogosult személy nyilatkozatot köteles aláírni arról, hogy a szabályzat tartalmát más, arra nem jogosult személlyel semmilyen formában nem osztja meg

5. Az Informatikai Biztonsági Szabályzat célja és hatálya

A szabályzat célja

A(z) **Tiszacsegei Közös Önkormányzati Hivatal** ASP rendszer alkalmazását vezeti be.

Jelen dokumentum célja az ASP rendszer által kezelt adatok biztonságának a megteremtése, továbbá az információbiztonsági követelményeknek való megfelelés biztosítása. A szabályzat összhangban áll 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.

A szabályzat egységes szerkezetbe foglalja a használatban lévő informatikai rendszerekkel és annak a felhasználóival szemben támasztott informatikai biztonsági követelményeket.

Az önkormányzat általános célú informatikai biztonságtechnikai szabályzata továbbra is érvényben marad.

Jelen dokumentum igyekszik kiküszöbölni minden lehetséges ellentmondást a Tiszacsegei Közös Önkormányzati Hivatal egyéb szabályzati és jelen szabályzat között. Amennyiben mégis előfordulna ilyen ellentmondás, abban az esetben az ASP rendszerre, annak alkalmazására, valamint az azzal kapcsolatba kerülő személyekre és tárgyi eszközökre vonatkozólag a jelen szabályzatban leírtak az irányadók, kivéve abban az esetben, amelyben az eredeti szabályozások szigorúbb feltételeket írnak elő, és nem akadályozzák az ASP rendszer szabályszerű működtetését.

Személyi hatálya

Az Informatikai Biztonsági Szabályzat kiterjed az önkormányzati szerv köztisztviselőire, ügyintézőire, a hivatal valamennyi munkatársára, valamint azokra a személyekre, akik részt vesznek az önkormányzatnál keletkező, tárolt, illetve továbbított adatok kezelésében (külső informatikai beszállító partnerek).

Tárgyi hatálya

Az Informatikai Biztonsági Szabályzat kiterjed az önkormányzatnál kezelt, keletkezett információkra, az informatikai rendszerben üzemeltetett valamennyi hardver és szoftver elemekre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja az önkormányzatnál keletkező, illetve felhasznált adatokat. Kiterjed továbbá a rendszerelemek dokumentációira. Mindezek kiterjednek a következőkre:

- az elektronikus adatok teljes körére, kivételek nélkül,
- a Tiszacsegei Közös Önkormányzati Hivatal tulajdonában lévő, illetve az általa használt valamennyi informatikai berendezésre,
- az alkalmazott szoftverekre, beleértve a rendszerszoftvereket és a hivatali munka során használt általános és egyedi programokat is,
- az informatikai eljárásokkal, eszközökkel, folyamatokkal kapcsolatos összes dokumentációkra, beleértve a belső utasításokat is,
- az adatok rögzítésére, tárolására, továbbítására, felhasználására vonatkozó utasítások dokumentációra, beleértve az adathordozók, mint elektronikus dokumentációtárolók tárolását, felhasználását, továbbítását is.

6. Szerepkörök, feladatok, felelősségek

Az informatikai biztonság megfelelő kialakításának egyik követelménye a biztonsággal kapcsolatos szerepkörök szétválasztása.

Az önkormányzat minden munkatársa, szerződésben lévő informatikai alvállalkozója és természetes személy köteles az Informatikai Biztonsági Szabályzat előírásait betartani.

A Tiszacsegei Közös Önkormányzati Hivatal által meghatározott informatikai biztonsági szerepkörök felsorolása a mellékletekben található.

7. Kapcsolódó eljárásrendek

A jogszabálynak történő megfelelés biztosítása érdekében az Informatikai Biztonsági Szabályzat mellett a Tiszacsegei Közös Önkormányzati Hivatal esetében az elektronikus információs rendszer legmagasabb osztályba sorolt értékéhez tartozó eljárásrendek listája a következő:

- Kockázatelemzési és kockázatkezelési eljárásrend
- Beszerzési eljárásrend
- Üzletmenet folytonosságra vonatkozó eljárásrend
- Biztonsági eseménykezelési eljárásrend
- Személybiztonsági eljárásrend
- Képzési eljárásrend
- Fizikai védelmi eljárásrend
- Biztonságelemzési eljárásrend
- Konfigurációkezelési eljárásrend
- Rendszer karbantartási eljárásrend
- Adathordozók védelmére vonatkozó eljárásrend
- Azonosítási és hitelesítési eljárásrend
- Hozzáférés ellenőrzési eljárásrend
- Rendszer és információ sértetlenségre vonatkozó eljárásrend
- Naplózási eljárásrend
- Rendszer- és kommunikáció védelmi eljárásrend

8. Informatikai Biztonsági Szabályzat kialakításához ASP specifikus irányelvek

Jelen egységesített dokumentumban, mint Egységesített Biztonságtechnikai Szabályzatban az ASP specifikus irányelvek összhangban vannak a Tiszacsegei Közös Önkormányzati Hivatal általános informatikai biztonságtechnikai irányelveivel.

9. Az ASP rendszerhez csatlakozás

A 257/2016. (VIII. 31.) Korm. rendelet 2. melléklete tartalmazza a minimumkövetelményekhez tartozó megfelelés elvárását.
Ez alapján került kialakításra az az informatikai infrastruktúra környezet, amelylyel biztosított az ASP rendszerhez történő csatlakozás, a következők fő komponensek alkalmazásával:

- munkaállomások beüzemelése,
- nyomtatók üzembe állítása,
- hálózati aktív eszközök beüzemelése, hálózat kiépítése,
- vírusvédelmi rendszer beüzemelése,
- tűzfal beüzemelése,
- internetkapcsolat üzembe állítása.

10. Az infrastruktúra felállítása

Az infrastruktúra felállítása során az alábbi feladatok végrehajtása szükséges minden esetben, valamint az egyes elemek meglétének folyamatos ellenőrzése, szükség esetén azonnali pótlása. A személyekkel kapcsolatos információk a biztonsági szerepkörök mellékletekben találhatók.

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

11. IT biztonsági feltételek megteremtése

- Önkormányzati biztonsági szint meghatározása a 23. pontban található, a hozzá kapcsolódó védelmi intézkedésekkel együtt.
- Az információbiztonsági szabályozások kialakítása, szükség szerinti módosítása, jóváhagyása, kihirdetése a 4. pontban foglaltak szerint.
- A Tiszacsegei Közös Önkormányzati Hivatal ASP-vel kapcsolatos, külső fél, szervezet által végzett audit tevékenységet nem tervez.
- Az ASP rendszeren a Tiszacsegei Közös Önkormányzati Hivatal nem tervez külső fél, szervezet által végzett sérülékenységi vizsgálatot.

12. Fizikai biztonság megteremtése ASP-ben

Az ASP-t futtató objektum tekintetében a Tiszacsegei Közös Önkormányzati Hivatal a következő intézkedéseket teszi meg:

- Az épület azon részeibe, ahol az ASP-t futtató objektumok (informatikai eszközök) találhatóak, illetéktelen személy ellenőrzetlenül nem léphet be, ott

nem tartózkodhat, az objektumokhoz nem férhet hozzá, valamint az adatokra (képernyőkre) passzív rálátással sem rendelkezik.

- Az épület kifejezetten az ASP-t futtató objektumokhoz tervezett és épített biztonsági rendszerrel nem rendelkezik. Az általános biztonsági intézkedések, tekintve a jelenlegi és a várható ügyfélforgalmat, várhatóan elegendő fizikai biztonságot jelentenek az informatikai adatvédelem szempontjából.

13. Őrzés, védelem

A fizikai biztonság megfelel a jogszabályi elvárásoknak.

Hivatali időn kívül az épületbe való bejutás csak jogosult személyek számára, speciális esetekben biztosított. Jogosulatlan személyek, idegenek az épületbe nem juthatnak be, valamint egy esetleges bejutás esetén sem férhetnek hozzá kritikus adatokhoz.

A védelmi rendszer biztonságát egyrészt a humán védelmi mechanizmus biztosítja, amely esetben a rendszer felhasználói a munkafolyamatok átmeneti felfüggesztése vagy befejezése esetében, a kilépési és lezárási folyamatok szabályos végrehajtásával gondoskodnak arról, hogy illetéktelen személyek az adatokhoz ne tudjanak hozzáférni. Az esetleges helyben tárolódó adatok (böngésző) automatikus eliminálásáról, kikapcsolás utáni hozzáférhetetlenségéről, a rendszergazda a szoftverek megfelelő beállításával gondoskodik.

Az épületben portaszolgálat működik, és így a munkaidőben az épületbe bejutás csak ellenőrzötten történhet. Az ASP-t futtató eszközök zárható munkaterületeken vannak elhelyezve, és a bejutás csak olyan esetben, és olyan módon történhet, ahol a jogosult személyek teljes rálátással rendelkeznek a környezetre vonatkozólag. Az esetlegesen szükséges incidenskezelés az általános irányelveknek és a helyi szokásoknak megfelelően történik.

Az önkormányzat törekszik a védelmi rendszer folyamatos javítására, a még biztonságosabb adatvédelmi szint elérésére és munkaköri biztonság folyamatos javítására.

14. Humán erőforrás az ASP-ben

A Tiszacsegei Közös Önkormányzati Hivatal a mellékletekben felsorolt módon szabályozza az ASP szakrendszer munkakörökhöz tartozó biztonsági követelményi felelősségeket és feladatokat.

A munkaköri alkalmassági vizsgálatokat az informatikai biztonsági szempontjából a Tiszacsegei Közös Önkormányzati Hivatal, mint munkáltató a kockázatokkal arányos módon, az általános eljárásrendje szerint szabályozza.

15. Oktatás, képzés az ASP-ben

A Tiszacsegei Közös Önkormányzati Hivatal működési területén az ASP rendszert csak olyan munkatársak alkalmazhatják, akik ASP oktatáson részt vettek, a használati követelményeket, és a program ismeretét megfelelően elsajátították, valamint a rendszert az elvárásoknak megfelelően, önállóan használni tudják.

A képzés során a biztonságtechnikai kérdéseket külön kell taglalni, és a jelen dokumentáció tartalmát az ASP-t alkalmazó felhasználókkal megismertetni, valamint ezek elfogadását az oktatási naplón aláírásukkal szükséges igazolni.

16. ASP jogosultság kezelés

A szerződésben meghatározott tenant adminisztrátorok rendszerbe történő „felvitelét" az ASP Központ végzi el az önkormányzat által megküldött adatlap alapján.

- A Tiszacsegei Közös Önkormányzati Hivatal szervezeti vezetője (Jegyző) jelen utasítása alapján a privilegizált joggal rendelkező felhasználók a munkatársaik részére további jogosultságot osztanak.
- A Tiszacsegei Közös Önkormányzati Hivatal fióknál (tenantnál) egy karbantartó személy van, a biztonsági szerepkörök mellékletekben megjelöltek szerint. Másik karbantartó kijelöléséig, és megfelelő ismereteinek megszerzéséig ez a jog nem vehető el. A karbantartó személy neve a mellékletben található „tenant adminisztrátor" címszó alatt.
- A rendszer használata során a privilegizált joggal rendelkező munkatársak a privilegizált jog használatát munkavégzésükhöz csak indokolt esetben használhatják.
- A privilegizált joghoz tartozó bejelentkezési azonosítót zárt borítékban, biztonságosan zárható helyen (páncélszekrényben) kell tárolni, és csak különleges esetekben (pl. haláleset, különösen hosszan tartó betegség stb.) szabad azt felbontani.

17. ASP rendszerbe történő belépés, authentikáció

A Belügyminisztérium – az Igazságügyi Minisztérium és a Nemzeti Adatvédelmi és Információszabadság hatóság bevonásával – megvizsgálta azt a kérdést, hogy az elektronikus személyi igazolvány (eSZIG) felhasználása az ASP rendszerbe történő azonosításra ütközik-e valamely jogszabályba, illetve szükséges-e az önkormányzat alkalmazásában álló közszolgálati tisztviselők jogszabályi kötelezése az eSZIG kiváltására. Ez nem ütközik jogszabályba.

Az ASP elsődleges autentikációs eszköze az eSZIG. A használatához javasolt kártyaolvasók hatóság által bevizsgált és elfogadott eszközök.

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 kell megkülönböztetett módon figyelni:

- Minden ASP rendszert használó munkatársnak rendelkeznie kell 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 vezetőjének a Jegyzőnek gondoskodnia kell arról, hogy a kérdéses kártya hiánya esetén az ASP rendszerbe történő ideiglenes bejelentkezés lehetősége biztosított legyen. Az ehhez tartozó szabályrendszer kialakítása elengedhetetlen.

18. Csatlakozó önkormányzatok kliens oldali biztonsága

Az ASP kapcsán kiemelten kell kezelni a csatlakozó önkormányzatokkal kapcsolatos biztonsági kockázatokat. A csatlakozó önkormányzatok a saját infrastruktúrájukat fogják használni az alkalmazások igénybevétele során, így a kliens rendszerek biztonsága nagymértékben befolyásolja a teljes ASP rendszer biztonságát. Fontos az ASP rendszerbe olyan kikerülhetetlen biztonsági megoldásokat beépíteni, ami szűkíti a felhasználók biztonságra kockázatos tevékenységének lehetőségét.

Az csatlakozó önkormányzatok tekintetében a lehetséges fenyegetettségek, sebezhetőségek, valamint ezek megelőzésére alkalmazható intézkedések 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, scriptek (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 (géplealllítás, 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.
	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.

Elem	Fenyegetések, veszélyek, sebezhetőségek	Védelem
	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 igénybe vett 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.
	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.

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

A fentiek értelmében a rendszer felelős gazdája (Oláh Ferenc rendszergazda) köteles gondoskodni az alábbiak lehetőségeiről, meglétéről, folyamatos üzemképességéről, rendelkezésre állásáról és/vagy üzemeltetéséről:

- Hozzáférés védelem beállítása.
- Vírusvédelmi rendszer alkalmazása, folyamatos frissítése.
- Böngészők biztonsági beállítása.
- Legújabb szoftver verziók, frissítések telepítése mind a rendszerprogramok, mind az alkalmazói programok esetében, rendszeres, automatikus frissítések keretében, vagy manuális telepítésekkel.
- A megfelelő naplózási folyamatok beállítása.
- Az előírt, és rendelkezésre álló fizikai védelmi eszközök alkalmazása.
- Követelményrendszer szerinti hozzáférés-védelem és rejtjelezés alkalmazása.
- Rejtjelezett adatátviteli csatorna használata.
- Hozzáférés-vezérlés kialakítása.
- Egyszer használatos jelszó.
- Hozzáférés-vezérlés kialakítása.
- Tűzfal-biztonságpolitika elkészítése, vagy aktualizálása.
- Biztonsági beállítások rendszeres ellenőrzése, naplózás, riasztás.
- Tűzfal biztonsági beállítása, adminisztrálása csak védett hálózatból vagy konzolról.
- Megfelelő hálózati biztonságpolitika, architektúra terv kialakítása.
- Hálózati végpont IP címhez, MAC címhez kötése.
- Minden jelentős biztonsági esemény naplózása, naplózott események folyamatos értékelése.

Szintén a fentiek értelmében a Tiszacsegei Közös Önkormányzati Hivatal felelős vezetője (Dr. Lajter Zoltán, Jegyző) köteles gondoskodni a következőkről:

- A fenti feladatokhoz szükséges anyagi erőforrások biztosítása.
- Csak megbízható forrásból származó program használatának biztosítása.

- Követelményrendszer szerinti fizikai biztonság kialakítása.

19. Munkaállomásra vonatkozó biztonsági elvárások

A Tiszacsegei Közös Önkormányzati Hivatal felelős informatikai szakmai vezetője (Oláh Ferenc rendszergazda) köteles gondokodni az ASP rendszerhez csatlakozó eszközök folyamatos karbantartásáról, változáskövetéséről a következők figyelembevételével:

- A folyamatot változáskövetési eljárásrendbe szükséges megfogalmazni.
- A munkaállomásokon legyen telepítve vírusvédelmi program, a legfrissebb vírus definíciós adatállománnyal. A végpontvédelem tartalmazzon e-mail (csatolmány) védelmet is.
- A munkaállomáson legyen megoldott a böngésző megfelelő biztonsági beállítása.
- Javasolt a tervszerű beavatkozásokhoz karbantartási időablak kijelölése.
- A munkaállomások programfrissítése elvárt, különös tekintettel a legfrissebben kiadott security patch komponensekre.
- A telepítő programok, a licensz azonosítók zárható helyen (páncélszekrény) legyenek tárolva.

A munkaállomások elhelyezésénél gondot kell fordítani:

- 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 legyen megoldott.
- Munkaidő végén a munkaállomások kikapcsolása történjen meg.

Az ASP központhoz csatlakoztatott infrastruktúra elemekre értelmezve javasolt:

- a naplóinformációnak a védelme,
- hiba esetén a naplóbejegyzések elemzése,
- a rendszer hozzáférés ellenőrzése.

20. Rosszindulatú kódok elleni védelem

Az ASP rendszerhez történő csatlakozás során elvárás, hogy az önkormányzatok a csatlakozó eszközök vírusvédelmét saját hatáskörben valósítsák meg.
A Tiszacsegei Közös Önkormányzati Hivatal esetében a vírusvédelmi rendszer kiépítése és folyamatos karbantartása, naprakészségének és működésének biztosítása a rendszerfelelős, Oláh Ferenc rendszergazda feladata.
A vírusvédelmi eljárások a szervezet méretére való tekintettel az általános informatikai szakmai szabályok szerint történnek.
A rendszerfelelős ezen kötelezettségének ellátásához szükséges eszközök folyamatos meglétéről a Tiszacsegei Közös Önkormányzati Hivatal gondoskodik.

21. Hálózatbiztonság, hálózatvédelem

A Tiszacsegei Közös Önkormányzati Hivatal informatikai hálózatán az ASP használatára vonatkozó szabályok és javaslatok figyelembevételével az alábbiakat határozza meg, és a feladatok ellátását a rendszerfelelős, Oláh Ferenc rendszergazda hatáskörébe utalja:

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra. Az új azonosítók zárt borítékban, és biztonságosan zárható helyen (páncélszekrény) legyenek tárolva. Csak előre kijelölt, privilegizált felhasználóknak legyen lehetősége bejelentkezni a kérdéses eszközökbe.
- A hálózativégpontok védelme legyen megoldva a lehetőségek figyelembevétele mellett.
- Az eszközök hálózatba történő illesztéséről készüljön dokumentáció.
- Az eszközök firmware frissítése a legutolsó stabil változatnak megfelelően történjen meg.
- A menedzselhető eszközök legfrissebb konfigurációja legyen elmentve és zárható helyen tárolva a fentieknek megfelelően.

Informatikai határvédelem, tűzfal

- A szervezet internethez való csatlakoztatása a központi tűzfalon keresztül történjen meg.
- A tűzfal szabályok dokumentálása és azok zárható helyen történő tárolása legyen biztosítva.

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

22. Mobil eszközök használata

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

- A mobil eszközök használatát minden esetben előzetes jegyzői engedélyezésnek kell megelőznie.
- A mobil eszközök (pl. notebook) használatára a munkaállomásokra vonatkozó szabályok is legyenek érvényesek.
- A gazdálkodási szabályzatban ki kell dolgozni a mobil informatikai eszközök igénylésének, kiadásának, visszavételének, nyilvántartásának üzemeltetésének a folyamatait, biztosítva azt, hogy a mobil eszközök illetéktelen kezekbe ne kerülhessenek.
- Továbbá azokat a szabályokat, amelyek az eszközök hivatalon kívüli kivitelére,az eszközök javítására, esetleges elvesztésére, vagy a selejtezésére vonatkoznak.

23. Osztályba sorolás eredménye

A 41/2015. (VII. 15.) BM rendelet értelmében az osztálybesorolás 2. szintű.

A szervezeti egységben nincsenek 2. biztonsági osztálynál magasabb besorolású rendszerelemek, ennélfogva az informatikai folyamatok részben szabályozottak. Ennek megfelelően az egyes elemekre vonatkozóan nincsenek egyedi szabályozások, hanem a működtetés az általános szabályozások szerint történik. Az elektronikai rendszerek kialakítására való törekvés állandó, de a rendelkezésre álló szakemberek és szaktudás a helyi lehetőségekhez igazított, és sem a szakembergárda, sem a rendelkezésre álló szaktudás nem mérhető össze a professzionális biztonságtechnikai szakemberek szaktudásával. Az elektronikus információs rendszerek biztonságával kapcsolatos szakmai feladatok egyetlen, általános informatikai szaktudással rendelkező, jogkörében korlátozott

személyhez vannak hozzárendelve. Az elektronikus rendszerek előállítanak olyan információkat, amelyek az informatikai biztonság hatáskörében kezelendők, de a hivatal, mint szervezet, ezeket az információkat nem elemzi. Az elektronikus biztonságra vonatkozó jelentések, a professzionális szakmai háttér hiánya miatt, annak ellenére nem teljes körűek, hogy a maximális informatikai biztonságra való törekvés állandó. Az informatikai beléptetési rendszer, a kezelt adatok védelme további fizikai intézkedéseket nem igényel.

Jegyző, a szervezet vezetője
Név: Dr. Lajter Zoltán

Feladatköre:
Felelős vezetőként gondoskodik az elektronikus információs rendszer védelméről az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény alapján:

- „11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:
- a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
- f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,
- g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
- h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
- i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
- k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
- n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
-

- 12. § A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:
- a) a 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
- b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
- c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére."

Elektronikus információs rendszer biztonságáért felelős személy
Név: Oláh Ferenc

Feladatköre:
Az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény alapján:

- „13. § (1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.
- (2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:
- a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.
- (3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.
- (4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.
- (5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését
- a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,
- b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők e törvény hatálya alá tartozó

elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

- (6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.
- (7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.
- (8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.
- (9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.
- (10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.
- (11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt."

A Tenant adminisztrátor feladatai:
Név: Oláh Ferenc

Feladatköre:
A Tenant adminisztrátor feladatköre az ASP rendszer használata során a következő:

- 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).

A Tenant felhasználók és vele kapcsolatba kerülő külső beszállítók feladatai:

maradéktalanul betartják jelen dokumentumban előírt szabályozókat, és az informatikai biztonságért felelős személyek (Dr. Lajter Zoltán Jegyző, Oláh Ferenc rendszergazda, ---Tenant adminisztrátor--- tenant adminisztrátor) informatikai biztonsággal kapcsolatos utasításait.