ECSÉD

Ecsédi Polgármesteri Hivatal

rendszerbiztonsági terve

Tartalomjegyzék

I. BEVEZETÉS

Az Ecsédi Polgármesteri Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), valamint annak végrehajtására kiadott rendeletekben foglalt elektronikus információbiztonsági feladatok elvégzésére irányuló felkészülést, illetve azok végrehajtását megkezdte.

Az Ibtv. 11. §-ának (1) bekezdés e) pontja és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 3.3.2.2. pontjában meghatározottak szerint az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, amely:

- összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával;
- meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;
- meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
- meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

- a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;
- meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;
- gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
- belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;
- frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- elvégzi a szükséges belső egyeztetéseket;
- gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Jelen dokumentum célja, hogy ismertesse a Hivatal rendszerbiztonsági tervét.

II. RENDSZERBIZTONSÁGI TERV

2.1. Az elektronikus információs rendszer hatóköre, biztosítandó szolgáltatásai, biztonsági követelmények

Személyi hatálya a Hivatallal közszolgálati jogviszonyban álló vezetőkre, ügyintézőkre, a munkaviszony keretében foglalkoztatott ügyviteli és fizikai alkalmazottakra, közszolgálati munkavállalókra terjed ki, valamint azokra a személyekre, akik részt vesznek az önkormányzatoknál keletkező, tárolt, illetve továbbított adatok kezelésében A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző felelős. A szabályzatot minden olyan személlyel ismertetni kell, aki az eszközök használatára engedélyt vagy utasítást kap. Erre új kollégák esetében az első munkanapon sort kell keríteni.

Tárgyi hatálya kiterjed a hivatal saját üzemeltetésű és kiszervezett informatikai rendszereiben működtetett valamennyi hardver berendezésre, szoftver elemre és ezek dokumentációira (fejlesztési, szervezési, programozási, műszaki, üzemeltetési, biztonsági) és az informatikai rendszerben feldolgozott adatállományok teljes körére. A központi szervek által üzemeltetett rendszerek védelmi intézkedéseit azok üzemeltetője biztosítja, illetve írja elő.

Területi hatálya kiterjed a hivatal székhelyére, telephelyére, továbbá mindazon objektumokra és helyiségekre, amelyekben a tárgyi hatály pontban meghatározott eszközöket, szoftvereket, adatokat vagy dokumentumokat hoznak létre, tárolnak, felhasználnak vagy továbbítanak.

Időbeli hatálya: a hatályba lépés napjától visszavonásig érvényes, felülvizsgálatát a szabályzatban meghatározottak szerint kell elvégezni.

A szabályzat előírásait alkalmazni kell a Hivatal belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat,

elektronikus szolgáltatások illetőleg dokumentumok esetében. A Hivatalban nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

2.1.1. Biztonsági követelmények

Jelen fejezetben kerülnek definiálásra azon biztonsági eljárások, szabályzati elemek, melyek a hivatal hálózatának használata során meghatározzák az egyes rendszerek, munkaállomások tekintetében azok használatának követelményeit összhangban az Informatikai Biztonságpolitikában megfogalmazott alapelvekkel.

Az informatikai rendszerben jogosultságrendszer működtetése útján kell gondoskodni arról, hogy az informatikai rendszerben tárolt programokhoz, adatállományokhoz, adatokhoz kizárólag ellenőrzött és dokumentált módon lehessen csak hozzáférni, és az illetéktelen hozzáférés, az adatolvasás, az adatmegsemmisítés, az adathamisítás megakadályozható legyen. Felelős: a megvalósításért a Rendszergazda, az ellenőrzésért az Információbiztonsági felelősnek.

Az Alkalmazásokban a felhasználói jogosultságok egyedi vagy szerepkör szinten történő megkülönböztetését kell előírni és azt nyilván kell tartani.

Egy hálózati szolgáltatáshoz hozzáférési jogot az a munkatárs kaphat:

- akinek munkavégzéséhez az adott szolgáltatás használata szükséges;
- aki rendelkezik az adott szolgáltatás biztonságos használatához szükséges szakmai, és információbiztonsági ismeretekkel;
- és biztonsági vagy egyéb okból (pl. összeférhetetlenség) nem esik korlátozás alá;
- az informatikai rendszer távolról történő eléréséhez kizárólag az Információbiztonsági felelős adhat jogot indokolt esetben.

A hivatal informatikai rendszerének távolról történő elérése VPN kapcsolattal lehetséges, melyhez külön jegyzői engedély szükséges.

Az automatikus felkapcsolódás lehetősége eshetőséget adhat jogosulatlan hozzáférésre alkalmazásokhoz is. Ezért a hivatal számítógéprendszerére eszközök

csatlakoztatását minden esetben engedélyezni kell. Az informatikai endszert lehetőség szerint úgy kell beállítani, hogy a nem engedélyezett eszközök ne kapcsolódhassanak a rendszerre.

Távdiagnosztikát végző hálózati csatlakozópontok (portok) hozzáférését ellenőrizni kell. Igen sok számítógépet és távközlő rendszert telepítenek úgy, hogy távdiagnosztikai képességeket is beállítanak a fenntartással foglalkozó mérnökök támogatására. Ha az ilyen távdiagnosztikát végző csatlakozópont védtelen, lehetőséget ad jogosulatlan hozzáférésre. Éppen ezért az ilyet védeni kell, olyan eljárással, amely szavatolni képes, hogy csak ellenőrzötten lehessen hozzáférni.

Az informatikai hálózatok túlnyúlnak egyes szervezeti egységeken, sokszor kiterjednek a szervezetek fizikai határain túlra is. Az integrált feladatok szükségessé teszik, hogy egy rendszerhez különböző szervezeti egységek, illetve szervezetek férjenek hozzá, illetve az egyes rendszerek összekapcsolását. Az ilyen kapcsolatok fokozhatják az informatikai rendszerekhez történő hozzáférések kockázatát, így meg kell teremteni a védelmét más szervezetek, vagy szervezeti egységek felhasználóitól.

A hálózatot, biztonságának megteremtése és ellenőrzése érdekében, szükség szerint különböző logikai hálózati tartományokra kell felbontani.

Fenti lehetőségeket a Rendszergazda veszi számításba a kockázatok esetleges csökkentése céljából.

Biztonságos bejelentkezési folyamattal kell lehetővé tenni a hozzáférést az informatikai szolgáltatásokhoz. Valamely számítógép-rendszerhez a belépési eljárást úgy kell kialakítani, hogy a jogosulatlan hozzáférés esélyét a minimálisra csökkentsük. A beléptető eljárásnak éppen ezért a rendszerrel csak a lehető legkevesebb információt szabad közreadni, hogy elkerülhessük, hogy a jogosulatlan felhasználót segítse.

Ahol a rendszer lehetővé teszi

- rendszer a belépés előtt a lehető legkevesebb információt szolgáltassa a technológiáról;

- sikertelen belépés esetén a rendszer nem jelölheti meg, hogy a megadott adatok mely része hibás;
- limitálni kell a sikertelen belépések számát és a belépési folyamat maximális idejét;
- limitálni kell a sikertelen belépések számát és a belépési folyamat maximális számát.

Az operációs rendszer szintjén elérhető biztonsági eszközöket arra kell használni, hogy korlátozzuk a hozzáférést a számítógép erőforrásokhoz.
Ezek az eszközök a következő képességekkel rendelkeznek:

- képesség az egyes jogosult felhasználók azonosságának, és szükség esetén munkaállomásának vagy telephelyének az azonosítására és igazolására;
- képesség a sikeres és a sikertelen rendszer hozzáférések rögzítésére;
- képesség a hitelesítés ellátására alkalmas eszközzel, és ha jelszógondozó rendszert alkalmaznak, akkor ez szavatolja a minőségi jelszavak használatát.

Az informatikai rendszer felhasználóitól meg kell követelni, hogy jelentsék a rendszerekben vagy a szolgáltatásokban minden felismert vagy feltételezett biztonsági eseményt, a rendellenestől eltérő működését. Ezeket haladéktalanul jelenteni kell vagy saját vezetőiknek, vagy az üzemeltetőnk, vagy az információbiztonsági felelősnek.
A biztonsági esemény kivizsgálása az információbiztonsági felelős feladata. A kivizsgálásba szükség esetén bevonhatja az üzemeltető munkatársait, illetve külső szakértőt.
Az informatikai rendszer minden üzemzavarát, elemeinek minden meghibásodását hibanaplóba kell bejegyezni.
A bejelentést fogadónak legalább a következőket kell feljegyeznie a bejelentett eseményekről: a bejelentés ideje, a bejelentő neve, az esemény rövid leírása, feltételezett oka, az elhárítás résztvevője, az elhárítás kezdete, az elhárításához megtett intézkedés, az elhárítás vége.

Az informatikai rendszer elemeinek meghibásodásairól vezetett bejegyzéseket rendszeresen értékelni szükséges.

Az informatikai rendszer felhasználóitól meg kell követelni, hogy jelentsék a rendszerek vagy a szolgáltatások minden felismert vagy feltételezett biztonsági gyengeségét vagy fenyegetettségét. Ezeket haladéktalanul jelenteni kell vagy saját vezetőiknek, vagy az üzemeltetőnek. A felhasználók a feltételezett gyengeséget semmilyen körülmények között se próbálják maguk megszüntetni.

A jelzett informatikai gyengeség kivizsgálása, a szükséges óvintézkedések meghatározása a Rendszergazda feladata. A kivizsgálásba szükség esetén bevonhatja az információbiztonsági felelőst.

A biztonsági események kezelésének felelősségeit és eljárásait úgy kell megállapítani, hogy a biztonsági eseményekre gyorsan, hatékonyan és rendben meg lehessen tennie a válaszlépéseket.

A következő védelmi intézkedéseket kell végrehajtani:

a napló állományokat és hasonló bizonyítékokat össze kell gyűjteni és azokat biztonságosan kell őrizni.

Az ismétlődő és jelentős hatású biztonsági eseményeket rendszeresen elemezni, értékelni kell és ezek alapján kiegészítő és továbbfejlesztett védelmi intézkedéseket kell bevezetni vagy a biztonsági szabályzat felülvizsgálati folyamatában, illetve a képzési tervben figyelembe venni a későbbi előfordulások gyakorisága, kára és költségei korlátozására.

Az informatikai biztonsági óvintézkedések kialakításakor törekedni kell arra, hogy az informatikai biztonság esetleges sérülése esetén a hivatal kellő bizonyítékkal rendelkezzen ahhoz, hogy indokolt esetben a bizonyíték támogasson egy intézkedést egy személy vagy más szervezet ellen.

Számítógép-adathordozón rögzített bizonyíték esetében a hordozható adathordozók, valamint a háttértárolón és a központi tárolón talált információ másolatait meg kell őrizni és rendelkezésre állásáról gondoskodni kell. Felelős az információbiztonsági felelős.

A másolási folyamat során valamennyi tevékenységről naplófeljegyzést kell elkészíteni és tanú jelenléte szükséges. A napló és az adathordozó egy-egy példányát biztonságosan meg kell őrizni.

2.1.2. Munkaállomásra vonatkozó biztonsági elvárások

Az ASP rendszerhez csatlakozó eszközök karbantartásáról, változáskövetéséről gondoskodni kell 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 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.

2.1.3. Rosszindulatú kódok elleni védelem

Az ASP rendszerhez történő csatlakozás során elvárás, hogy az önkormányzatok a csatlakozó eszközök vírusvédelmét saját hatáskörben valósítsák meg.
A vírusvédelmi eljárások követelményei

- Meg kell határozni a vírusfertőzés megelőzésére vonatkozó szabályokat. Például: Működő vírusvédelmi rendszer nélkül munkaállomást, laptopot, számítógépes hálózatot nem szabad üzemeltetni. Továbbá a vírusvédelmi program vírus definíciós állományit a legfrissebb állapotba kell tartani.
- A teendőket rögzíteni kell vírusfertőzés esetén.
- Vírustámadás esetén szükség szerint a vírusriadó elrendelése.
- Sérülés, vírusfertőzés után az elvárt helyreállítási eljárások meghatározása.

2.1.4. Hálózatbiztonság

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

- A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra. Legyen megoldott az azonosítók zárt borítékban, és biztonságosan zárható helyen történő tárolása. Csak előre kijelölt, privilegizált felhasználóknak legyen lehetősége bejelentkezni a kérdéses eszközökbe.

- A hálózati végpontok védelme legyen megoldva. A lehetőségek figyelembevétele mellett pl. port security, esetleg 802.1x szabványnak megfelelően.
- 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.

Informatikai határvédelem, tűzfal

- A szervezet internethez való csatlakozástatása 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.

2.1.5. 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 érvényesek.
- Ki kell dolgozni 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.

2.2. Az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztálya

Annak érdekében, hogy az adatkezelő által használt és az Ibtv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából. Az adatkezelő által használt elektronikus információs rendszerek biztonsági osztályba sorolása határidőben megtörtént, az külön dokumentumot képez.

A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A soron kívüli biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni.

A soron kívüli felülvizsgálatot akkor is el kell végezni, ha a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

Az elektronikus információs rendszerek osztályba sorolásának az eredményét az Informatikai Biztonsági Szabályzatban rögzíteni kell. Jelen esetben ennek az értéke a következő:

Szakrendszer	Biztonsági osztály
Adó rendszer	4
Keretrendszer	4
Gazdálkodási rendszer	3

2.3. Az elektronikus információs rendszer működési körülményei és más elektronikus információs rendszerekkel való kapcsolatai

2.3.1. Harmadik fél hozzáférési biztonsága

A harmadik fél számára adható hozzáférés fajták a következők:

- fizikai hozzáférés (a hivatalhoz, számítógépteremhez, tároló szekrényhez);
- logikai hozzáférés (a hivatal adatbázisaihoz, informatikai rendszerhez).

A külső felek számára biztosított hozzáférés esetén hozzáférések okai a következők:

- a hardver és a szoftver támogatók személyzete, akiknek rendszerszintű vagy legalább is alsószintű hozzáférésre van szükségük;
- társszervezetek, amelyek információt cserélhetnek, amelyek hozzáférhetnek az informatikai rendszerhez vagy osztozhatnak a közös adatbázison.

Azon külső felek, amelyek szerződésükben meghatározott módon a helyszínen végeznek munkát, ugyancsak biztonsági kockázatot jelentenek. A helyszínen munkát végző külső felek lehetnek:

- hardvert és szoftvert karbantartó és támogató személyzet;
- tisztító-, ellátó-személyzet, biztonsági őrség, valamint hasonló erőforrás-kihelyezést támogató szolgáltatások;
- eseti, rövididejű alkalmazottak;
- konzultánsok;
- ellenőrző szervezetek munkatársai.

Minden külső fél által végzett munkavégzés esetében előzetesen kockázatfelmérést kell végezni, é a titoktartási nyilatkozatot az érintett felekkel alá kell íratni. A kockázatfelmérést a megbízó vezető végzi, amennyiben az informatikai rendszerhez való hozzáféréshez is szükség van abban az esetben az Információbiztonsági felelős bevonásával.

A kockázatfelmérés során figyelembe kell venni az elvárt hozzáférés fajtáját, az információ értékét, a külső fél által használt óvintézkedéseket, valamint a hivatal

információihoz történő hozzáférés hatását a biztonságra. A kockázatfelmérés alapján, amennyiben szükséges további külön óvintézkedéseket kell meghatározni és alkalmazni. Az informatikai rendszert érintő óvintézkedésekért az Információbiztonsági felelős felel.

2.3.2. A harmadik féllel kötött szerződés biztonsági következményei

A hivatal információ-feldolgozó rendszereihez harmadik fél hozzáférési lehetőségét a féllel kötendő hivatalos szerződésbe bele kell foglalni. A szerződés tartalmazza, vagy utal minden olyan informatikai biztonsági követelményre, amely biztosítja a hivatal biztonsági szabályzatának és a szabványoknak való megfelelést.
A szerződésnek kell szavatolnia azt is, hogy semmilyen félreértés ne maradjon a harmadik fél és a hivatal között. A következő információkat kell a szerződésbe foglalni:

- az informatikai biztonsági szabályzatra való hivatkozást;
- vagyonvédelmet, beleértve:
- a hivatal vagyonának a védelmét, beleértve az információvagyont és a szoftvert is;
- az óvintézkedéseket, amelyek biztosítják, hogy a szerződés lejáratával vagy a szerződés érvényességi idején belül egy előre meghatározott időpontban, az átadott információkat vagy megsemmisítik, vagy pedig visszaszolgáltatják;
- az információ másolatának és nyilvánosságra hozatalának korlátozásait;
- valamennyi rendelkezésre bocsátandó szolgáltatás leírását;
- a hivatal informatikai rendszeréhez történő hozzáférés esetén a megengedett hozzáférés módokat;
- a felhasználói tevékenységek megfigyelésének jogát.

A harmadik féllel (alvállalkozóval) a többi feltétel és körülmény mellett meg kell ismertetni az IBSZ-ben foglaltak rá vonatkozó követelményeit is. Ezért a szervezet vezetője felelős.

III. ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2017. július 3. napján lép hatályba és visszavonásig érvényes.

Ecséd, 2017. július „3"

ECSÉDI POLGÁRMESTERI HIVATAL Jegyző Ecséd

Nagy Lászlóné

jegyző