ECSÉD

Ecsédi Polgármesteri Hivatal

Informatikai Biztonsági Szabályzata kiegészítése

a 77/2013. (XII.19.) NFM rendelet, valamint az informatikai kockázatértékelés és biztonsági osztályba sorolás alapján

2014.

I. BEVEZETÉS

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 11. § (1) bekezdés f) pontjában kapott felhatalmazás alapján a szervezet informatikai biztonsági szabályzatát a következők szerint egészítem ki:

1.1. A SZABÁLYZAT CÉLJA, HATÁLYA, FELÜLVIZSGÁLATA

A szabályzat célja az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása érdekében felmerülő feladatok és felelősök meghatározása.

Az Ecsédi Polgármesteri Hivatal, mint adatkezelő szervezet által használt elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

- az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
- az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása
- zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

Az informatikai biztonsági szabályzat felülvizsgálatára 3 évente kell sor kerülnie, illetve soron kívüli felülvizsgálat, frissítés szükséges:

- jogszabályváltozás,
- szervezeti átalakulás,

- információbiztonsági felelős személyében bekövetkezett változás,
- NEIH jelzése esetén.

Az informatikai biztonsági szabályzat tárolásáról a jegyző gondoskodik zárható lemezszekrényben ezáltal megakadályozva a jogosulatlan hozzáférést.

A szabályzat módosításának kezdeményezésére jogosult:

- jegyző,
- információbiztonsági felelős,
- NEIH.

II. A SZERVEZET VEZETŐJÉNEK FELADATAI

Az Ecsédi Polgármesteri Hivatal Jegyzője köteles gondoskodni az elektronikus információs rendszerek védelméről, amely körében:

- biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
- kiadja a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonságpolitikáját,
- meghatározza a szervezet elektronikus információs rendszereinek informatikai biztonsági stratégiáját,
- meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
- rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
- gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- 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,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek,
- ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
- megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket,
- ellátja a vonatkozó jogszabályokban meghatározott egyéb feladatait.

A szervezet vezetője együttműködik az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatósággal, amely során a hatóság részére:

- az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,

- a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
- az ellenőrzés lefolytatásához szükséges feltételeket biztosítja.

III. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER BIZTONSÁGÁÉRT FELELŐS SZEMÉLY

A szervezet vezetője a II. pontban és a vonatkozó jogszabályokban meghatározott feladatainak előkészítése és végrehajtása céljából elektronikus információs rendszer biztonságáért felelős személyt nevez ki. Az elektronikus információs rendszer biztonságáért felelős személy kinevezése során tekintettel kell lenni az Ibtv. 13. § (7)-(10) bekezdésében foglaltakra.

Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

- gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, elvégzi vagy irányítja ezen tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,

- kapcsolatot tart az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatósággal és a kormányzati eseménykezelő központtal,
- az Ibtv. hatálya alá tartozó bármely elektronikus információs rendszert érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet,
- részt vesz a vonatkozó miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen,
- előkészíti a szervezet vezetőjének a vonatkozó jogszabályokban szereplő egyéb feladatait,
- ellátja a vonatkozó jogszabályokban meghatározott egyéb feladatait.

A fenti feladatok és felelősségek más személyre át nem ruházhatók.

IV. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI OSZTÁLYBA SOROLÁSA[1]

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 sorolás elkészítéséért felelős: **információbiztonsági felelős**

[1] A biztonsági osztályba sorolás követelményeit a 77/2013. (XII. 19.) NFM rendelet 1. számú melléklete tartalmazza. A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni.

A biztonsági osztályba sorolást jóváhagyja: **jegyző**

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.

A biztonsági osztályba sorolás felülvizsgálatáért felelős: **információbiztonsági felelős**

Ha a felelős az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet készít a hiányosság megszüntetésére.

A cselekvési terv előkészítéséért felelős: **információbiztonsági felelős**

A cselekvési terv jóváhagyásáért felelős: **jegyző**

V. AZ ECSÉDI POLGÁRMESTERI HIVATAL BIZTONSÁGI SZINTJE

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján biztonsági szintje:[2] 0

[2] A szervezet a 77/2013. (XII. 19.) NFM rendelet 2. számú mellékletében meghatározott szempontok alapján meghatározza, hogy melyik biztonsági szintnek felel meg.
A szervezet biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai esetében legalább 2.

A biztonsági szintbe sorolás alapjául szolgáló vizsgálat lefolytatásáért felelős: **információbiztonsági felelős**

A biztonsági szintbe sorolás jóváhagyásáért felelős: **jegyző**

A biztonsági szint meghatározását legalább háromévenként, szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

A biztonsági szint meghatározásának felülvizsgálatáért felelős: **információbiztonsági felelős**

Cselekvési terv elkészítéséért felelős: **információbiztonsági felelős**

A biztonsági szintbe sorolás jóváhagyásáért felelős: **jegyző**

Biztonsági helyzet és esemény értékelésért felelős: **információbiztonsági felelős**

Értékelés alapján szükséges intézkedés megtételéért felelős: **jegyző**

VI. LOGIKAI, FIZIKAI ÉS ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

Az elektronikus információs rendszerek védelme körében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 77/2013. (XII. 19.) NFM rendeletben előírt logikai, fizikai és adminisztratív védelmi intézkedések meghatározása az információbiztonsági felelős feladata.

Az intézkedéseknek támogatni kell a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, a biztonsági események kezelését.

Az intézkedések előkészítéséért, végrehajtásáért a jegyző mint a szervezet vezetője a felelős.

Az elektronikus információs rendszer (ideértve azok elemeit is) és információtechnológiai szolgáltatás beszerzés szabályait a beszerzési eljárásrend szabályozza.

Biztonsággal kapcsolatos tervezésre (pl: beszerzés, fejlesztés, eljárásrendek kialakítása) javaslattételre jogosult az információbiztonsági felelős.
Javaslat végrehajtásáért felelős a jegyző.

Az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében a képzési eljárásrendben szabályozott.

A rendszerelemekben a fejlesztők által javasolt, illetve előírt változásokat a rendszergazda köteles 3 munkanapon belül végrehajtani.
Az üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása) az informatikai katasztrófa elhárítási tervben került rögzítésre.

Az érintett szervezetnek nincs lehetősége arra, hogy a rendszerek használatáról szóló rendszerbejegyzések értékelje, az értékelés eredményétől függő eljárásokat meghatározza.

A hivatali munkaterületen (az elektronikus információs rendszerhez hozzáférve) csak a jegyző, a hivatali alkalmazottak és a jegyző által kiadott, névre és meghatározott időre szóló engedéllyel rendelkező személyek tartózkodhatnak.

A beléptetési engedélyekről naprakész nyilvántartást kell vezetni, egy külön erre a célra rendszeresített hitelesített füzetben, amelyben az alábbi adatoknak kell szerepelnie:

- a belépésre jogosult neve,
- a munkáltatója neve (cég/vállalat),
- a belépés pontos dátuma (év, hó, nap, óra), hosszabb távra kiadott engedély esetén a kezdő és lejárat dátum,
- a belépés célja (karbantartás, ellenőrzés),
- a fogadó személy neve, beosztása,
- az engedély kiállítási dátuma,
- az engedélyező aláírása,
- az engedély nyilvántartási száma.

VII. ZÁRÓ RENDELKEZÉSEK

A szabályzat kiegészítés 2014. december 1. napján lép hatályba.

A Jegyzőnek kell gondoskodni, hogy a szabályzatban foglalt előírásokat az érintett munkatársak megismerjék, annak tényét a szabályzat ***1. számú mellékletében*** szereplő megismerési nyilatkozaton aláírásukkal igazolják a hatálybalépés napjával egyidejűleg.

Az érintett dolgozók munkaköri leírásában szerepeltetni kell a szabályzatban nevesített felelősségi, hatás- és jogköröket, melyek elkészítéséért a jegyző a felelős.

Ecséd, 2014. december „10" „.

ECSÉDI POLGÁRMESTERI HIVATAL Jegyző Ecséd

a.l. jegyző