ECSÉD

Ecsédi Polgármesteri Hivatal

konfigurációkezelési eljárásrendje

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 3.3.6.1. pontjában meghatározottak szerint az Konfigurációkezelési eljárásrendben a Hivatal mint érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő; a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

Jelen dokumentum célja, hogy ismertesse a Hivatal konfigurációkezelési eljárásrendjét.

II. KONFIGURÁCIÓKEZELÉS

2.1. Konfigurációkezelési eljárásrend

Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő; a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

2.2. Alapkonfiguráció

Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

Az érintett adminisztrátorok és adatgazdák az információbiztonsági felelős közreműködésével elektronikus információs rendszereikhez egy-egy alapkonfigurációt fejlesztenek ki, dokumentálják és karbantartják azt, leltárba foglalva annak lényeges elemeit. A Szervezet:

- az elektronikus információs rendszert úgy konfigurálja, hogy az *csak a szükséges szolgáltatásokat nyújtsa*;

- meghatározza *a tiltott, vagy korlátozott, nem szükséges funkciók*, portok, protokollok, szolgáltatások, szoftverek használatát.

A Szervezet:

- meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon – a „szükséges minimum" elv alapján
- az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;
- elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
- a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;
- figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, a szervezet belső szabályzataival és eljárásaival összhangban.

2.3. A konfigurációváltozások felügyelete (változáskezelés)

Az érintett szervezet

- meghatározza a változáskezelési felügyelet alá eső változástípusokat; meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.);
- megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja vagy elutasítja azokat;
- dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;

- megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;

- visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;

- auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

2.4. Előzetes tesztelés és megerősítés

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

2.5. Biztonsági hatásvizsgálat

Az érintett szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.

2.6. Konfigurációs beállítások

Az érintett szervezet meghatározza a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon - a „szükséges minimum" elv alapján - az elektronikus információs rendszerben használt

információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja; elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést; figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett szervezet belső szabályzataival és eljárásaival összhangban.

2.7. Legszűkebb funkcionalitás

Az érintett szervezet az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa; meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

2.8. Elektronikus információs rendszerelem leltár

Az érintett szervezet leltárt készít az elektronikus információs rendszer elemeiről; meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;gondoskodik arról, hogy a leltár pontosan tükrözze az elektronikus információs rendszer aktuális állapotát; az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza; legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez. Az érintett szervezet az elektronikus információs rendszerelem leltárt frissíti az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában *(Lásd külön dokumentumban:* ***elektronikus információs rendszerelem leltár****).*

2.9. A szoftverhasználat korlátozásai

Az érintett szervezet kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak; a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát; ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

A Szervezet bármely informatikai rendszerére csak a rendszergazda és munkatársai telepíthetnek szoftvert, ***a felhasználónak szoftvertelepítésre és bizonyos beállítások módosítására nincs sem joga, sem lehetősége.*** A Szervezet informatikai eszközeire TILOS illegális és/vagy nem jogtiszta szoftvert telepíteni! A Szervezet informatikai infrastruktúrájában a feladatok végrehajtására kizárólag a Szervezet által megvásárolt licencű kereskedelmi szoftver termékeket és/vagy szabad szoftvereket lehet alkalmazni. Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből. Ezt a műveletet a felhasználó tudtával és az információbiztonsági felelős engedélyével a rendszergazda végzi el.

Illegális szoftverek használata esetén a felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat.

A telepítést megelőzően a szervezetben vírusvédelmi célokra üzembe állított eszközzel meg kell vizsgálni a szoftver esetleges vírusfertőzöttségét. Amennyiben technikailag/technológiailag lehetséges, úgy az új szoftvercsomagról biztonsági másolatot kell készíteni. Az installálást csak a munkapéldányról szabad végezni. Az eredeti példányt biztonságos helyen kell tárolni.

A Szervezet infrastruktúrájában található eszközökre idegen program, adat másolása tilos!

Lásd részletesen Informatikai Biztonsági Szabályzat XIII. fejezet !

2.10. A felhasználó által telepített szoftverek

Az érintett szervezet megfogalmazza az elektronikus információs rendszer vonatkozásában, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségét; érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint; meghatározott gyakorisággal ellenőrzi a szabályok betartását.

A felhasználók az informatikai eszközöket Szervezeti munkavégzés céljára kapják. A felhasználók jogosultsága a belső hálózaton csak az informatikai üzemeltetésért felelős szervezeti egység által telepített egységes irodai alkalmazások és szolgáltatások használatára, illetve a munkájukhoz szükséges alkalmazói programok futtatására terjed ki. A Szervezet informatikai infrastruktúráját magán célú használatra igénybe venni TILOS!

Ettől eltérni csak a szervezet vezetője vagy a információbiztonsági felelős engedélyével, akkor is kizárólag mobil eszközök esetében szabad (notebook, tablet, mobiltelefon, mobil adathordozók). Az engedély feltétele felhasználói nyilatkozat tétele arról, hogy az adott felhasználó - a tűzfallal leválasztott nyilvános részek (pl. free „vendég" wifi) kivételével - nem használja a szervezet belső informatikai struktúráját. Ebben az esetben a felhasználót kockázatokról tájékoztatni kell, aki a nyilatkozat tételével lemond a szervezet nem nyilvános hálózatának bármilyen használati lehetőségéről és a kivont eszköz hardver és szoftver karbantartását is átvállalja. Karbantartási kötelezettsége nem terjed ki garanciális javítás ügyintézésére, azt továbbra is a rendszergazda feladata.

Lásd részletesen Informatikai Biztonsági Szabályzat XIII. fejezet !

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