RAGÁLYI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGPOLITIKA

Verziószám: 1.0

Dátum: 2021.01.18.

Tartalomjegyzék

1. Általános rendelkezések

1.1. Az intézkedés célja

a) Az Informatikai Biztonságpolitika (a továbbiakban: IBP) a Hivatal vezetésének akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információs vagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetésére, megfelelés a 2013. évi L. törvénynek (az állami és önkormányzati szervek elektronikus információbiztonságáról).

b) Az IBP célja irányelveket adni a biztonságért felelős vezetők részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntéseik meghozatalához, továbbá az elektronikus információs rendszerek rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

1.2. Az intézkedés hatálya

a) RAGÁLYI KÖZÖS ÖNKORMÁNYZATI HIVATAL (a továbbiakban: Hivatal). valamint a Szervezeti és Működési Szabályzat szerinti szervezeteire.

b) A Hivatal és szervezetei valamennyi vezetőjére, ügyintézőjére, a rendszerek felhasználóira, üzemeltetőire.

c) A Hivatallal és szervezeteivel külső, megbízásos (szerződéses) eseti munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a fenti szerződések tartalmának megfelelő kialakításával kell biztosítani.

d) A Hivatal és szervezetei által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a keletkező, illetve felhasznált adatokat, információkat.

2. Informatikai Biztonságpolitikával kapcsolatos alapelvek

2.1. Információvédelem területei

A 41/2015. (VII. 15.) BM rendeletben megfogalmazott elvárásoknak azon fejezetei, amelyek kielégítik a Hivatalra vonatkozó biztonsági osztályba sorolási szintet.

2.2. Az Informatikai Biztonságpolitika a Hivatal szolgálatában

a) A Hivatal és szervezetei kezelésében, valamint felügyeletében működő és ezeket az intézményeket kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellégére és biztonságára vonatkozó törvényeknek megfelelően kell üzemeltetni.

b) Az informatikai rendszerekben adatot, információt és egyéb szellemi tulajdont az intézmény számára jelentkező értékével arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a sérüléstől, megsemmisüléstől és a nyilvánosságra kerüléstől. A védelemnek biztosítani kell az informatikai rendszer megbízható működését fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén. A biztonsági szabályok megsértése esetén az IBP hatálya alá eső személyekkel szemben felelősségre vonási eljárást kell kezdeményezni.

c) A védelem megvalósítása érdekében a tervezés során a költségvetésben biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika,

valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

2.3. Az Informatikai Biztonságpolitika helye az informatikai biztonsággal foglalkozó dokumentumok rendszerében

a) A Hivatal és szervezeteinek vezetői az informatikai rendszerek, illetve rendszerelemek teljes életciklusára, az informatikai biztonság elviselhető kockázati szinten tartása érdekében kialakítják (szükség szerint külső segítség igénybevételével) az informatikai biztonsági dokumentációs rendszert.

b) A Hivatal és szervezetei informatikai biztonságával kapcsolatos szabályokat és elvárásokat az informatikai biztonsági dokumentációs rendszer tartalmazza, úgymint:

- törvényi előírások és egyéb jogszabályok,
- biztonsági iránylevek, eljárások,
- az Informatikai Biztonságpolitika,
- az Informatikai Biztonsági Szabályzat,
- alsóbb szintű informatikai biztonsági szabályzatok, eljárásrendek
- rendszerbiztonsági tervek (üzletmenet-folytonosság, mentés, naplózás)
- biztonsági nyilvántartások, sémák, tervek, vázlatrajzok, űrlapok.

c) Az informatikai biztonsági feladatok végrehajtásához szükséges feltételek megteremtését az informatikai biztonsági stratégiában szerepeltetni kell.

2.4. A biztonságpolitikai alapelvek és védelmi célkitűzések

A Hivatal és szervezetei az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánják következetesen érvényesíteni:

a) Bizalmasság biztosítása a Hivatal és szervezetei által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók kezelése, valamint a kommunikáció során.

b) Sértetlenség biztosítása a Hivatal és szervezetei teljes adatvagyonára vonatkozóan az adatkezelés, adattárolás és a kommunikáció során.

c) A Hivatalnál és szervezeteinél történő adatkezelések és feldolgozások során követelmény, hogy a pontos és helyes információkat dolgozzák fel, az adatok sértetlenségét megőrizzék a feldolgozás előtt, közben és után.

d) Rendelkezésre állás fenntartása elsősorban a Hivatal és szervezetei adatvagyonára vonatkozóan, amelyet biztosítani kell mind a külső, mind pedig a belső adatkérések során.

e) Működőképesség fenntartása a Hivatal és szervezetei informatikai rendszereire és rendszerelemeire vonatkozóan, amely az adott informatikai eszköz vagy rendszer elvárt és igényelt üzemelési állapotban való fennmaradását jelenti. Ennek elérése céljából biztosítani kell a megfelelően képzett személyzetet és technikai feltételeket.

3. Tartalmi követelmények

3.1. A Hivatal és szervezeteinek vezető beosztású tagjainak elkötelezettsége

a) A Hivatal és szervezetei önállóan alakítják ki informatikai biztonsági szabályrendszerüket, azonban ezen szabályok nem mondhatnak ellent a vonatkozó törvényi előírásoknak és az Informatikai Biztonsági Politikájának.

b) A Hivatal megfogalmazza az Informatikai Biztonsági Szabályzat, és további kötelezően előírt szabályzatok készítésének alapelveit, amely alapelvek alapján a hivatal és az intézmények elkészítik saját informatikai biztonsági szabályzatukat a saját, működő rendszerük tekintetében.

c) A Hivatal és szervezetei informatikai kapcsolatainak kialakítására illetve biztosítására csak olyan technikai és adminisztratív intézkedések engedélyezhetők, ill. valósíthatók meg, amelyekkel a jogszabályi és egyéb előírásoknak megfelelően biztosítják az informatikai rendszereik védelmét.

3.2. A Hivatal és szervezetei informatikai biztonságának területeire vonatkozó alapelvek és követelmények

3.2.1 Az adminisztratív és fizikai védelemi feladatok tekintetében

a) A Hivatal a rendeletnek megfelelően kialakítja az elvárt dokumentációs rendszert, köztük a politikát, célokat és terveket alkot, és olyan nyilvántartásokat vezet be és tart fenn, amely alapja egy pontos és helyes szakmai kockázatelvű vizsgálatnak.

b) Kockázatelemzést végez a veszélyek, fenyegetettségek feltérképezésére és az intézkedések sorrendjének gazdasági megalapozására.

c) Terveket alkot az elvégzendő feladatok követésére.

d) Felügyeli a rendszer és szolgáltatás beszerzését, engedélyezését.

e) Informatikai biztonsággal kapcsolatos feladatkörök meghatározása.

A felső vezetésnek a szervezeten belül, hogy a dolgozók csak a munkakörükhöz, illetve beosztásukhoz tartozó feladatokat lássák el. Mindenkit tájékoztatni kell arról, hogy milyen mértékű belső ellenőrzési és biztonsági felelősséggel tartozik.

f) Informatikai biztonsági szervezet informatikai biztonsági tervezése, alapkövetelményeinek lefektetése, bevezetése és ellenőrzése a szervezet vezetőinek a feladata.

A vezetők igénybe vehetnek biztonsági szakértőket annak érdekében, hogy megfelelő információkkal rendelkezzenek a szervezetük informatikai biztonsági helyzetéről. A szakértők feladata továbbá, hogy gondoskodjanak a különböző szabványok és ajánlások alkalmazásáról. A vezetők igénybe vehetik a szakértőket a biztonsági események kivizsgálása és értékelése során is.

g) Személyekre vonatkozó biztonsági megállapításoknál a Hivatal és szervezeteinél az informatikai biztonsági követelmények és annak betartásának követelményeit a dolgozóval ismertetni kell, ezért az Informatikai Biztonsági Szabályzatban részletesen szabályozni kell a következő területeket:

- informatikai funkciók meghatározása,
- munkavállalókkal szembeni követelmények,
- titoktartási nyilatkozatok.

h) Illetéktelen hozzáférés megakadályozása, továbbá a Hivatalnál és szervezeteinél az infrastrukturális elemek (pl.: kábelhálózat, szerverszobák) kialakítása során figyelembe kell venni az Informatikai Biztonsági Szabályzatban meghatározott szempontokat is.

i) Az informatikai rendszer környezeti feltételeinek biztosítása.

Az informatikai rendszerek külső környezeti hatásoktól való védelme úgy, hogy a szervezet vagyona és az ügymenet folytonossága ne legyen veszélyeztetve.

A védelemnek biztonsági osztályba sorolástól függően ki kell terjednie a biztonságos elektromos ellátás a klimatizálás, a tűz- és villámvédelem biztosítására is.

j) Adminisztratív védelem aktualizálása, karbantartása úgy, hogy az informatikai rendszerben bekövetkezett változásokat és alkalmazott problémakezelési eljárásokat (tervezés, létrehozás, üzemeltetés-karbantartás, megszüntetés) dokumentált formában, a szabályozó előírásoknak megfelelően kell végezni.

Az informatikai biztonsági dokumentációs rendszer aktualitásának fenntartása érdekében a rendszerben található dokumentumok rendszeres karbantartást igényelnek.

A dokumentációs rendszer dokumentumait felül kell vizsgálni a következő esetekben:

- a szervezet igényei, céljai megváltoznak,
- új területek, szolgáltatások jelennek meg,
- informatikai szolgáltatások szűnnek meg,
- új informatikai technológiák kerülnek bevezetése,
- informatikai technológiák alkalmazása szűnik meg,
- a kockázatelemzés következtében új, lényeges változtatások válnak szükségszerűvé.

k) Oktatás, képzés és a biztonságtudatosság fokozása

A Hivatal és szervezetei az informatikai biztonsági dokumentációs rendszerben foglaltaknak megfelelően. Ennek érdekében fontosnak tekintjük az informatikai biztonsági képzést, oktatást, az informatikai biztonság tudatosítását.

A biztonsági követelmények maradéktalan teljesülése érdekében oktatást, képzést kell biztosítani minden informatikai szereplő számára az informatikai biztonságtudatosságának fejlesztésével kapcsolatban, valamint a rendszerek üzemeltetéséhez és rendeltetésszerű használatához szükséges biztonsági követelmények elsajátítása érdekében.

3.2.2 A logikai védelemi feladatok tekintetében

a) Számítógép-hálózati biztonságánál a Hivatal és szervezetei az informatikai rendszereiket logikai, technikai és adminisztratív eszközökkel védik a külső kapcsolatok, egyéb szervezetek és az Internet felől érkező támadások ellen.

b) Hozzáférés szabályozás

A Hivatalnál és szervezeteinél a felhasználók csak ellenőrzött körülmények között, a szükséges felhasználói jogosultságokkal férhetnek hozzá az informatikai rendszerekhez és szolgáltatásokhoz. A külső felek nem férhetnek hozzá a számítógépes rendszerekhez, számítógépekhez.

A hozzáférések szabályainak kialakításánál a felhasználói profilokat rendszerenként kell meghatározni a szükségesnél nem több hozzáférési jogosultság elve alapján és ehhez kell a személyeket hozzárendelni.

A felhasználói hozzáférések kezelésére szóló eljárást a felhasználónak a rendszerbeli teljes életciklusán keresztül kell érvényesíteni. (Az új felhasználók felvételétől, a felhasználó kilépéskor történő jogosultságainak megszüntetéséig.)

c) Adattovábbítás elektronikus úton a bizalmas tranzakciók adatainak cseréje a jogszabályokban meghatározottak szerint csak megbízható csatornákon történhet.

A bizalmas információk közé tartoznak a biztonsági eljárásokhoz kapcsolódó információk, a bizalmas tranzakciók adatai, a jelszavak és a kriptográfiai kulcsok. Ezek továbbítására a hagyományos eljárási rend, illetve elektronikus úton való továbbításukhoz megbízható csatornák kialakítására van szükség, amely a különböző felhasználók és a rendszerek, valamint a különböző rendszerek közötti rejtjelezéssel valósítható meg.

d) Adatok sértetlenségének, konzisztenciájának biztosítása

Az adatok bevitele során biztosítani kell a forrás dokumentumok, az adatbeviteli munkakörök és munkaállomások biztonságát és azonosíthatóságát, valamint a bevitt adat ellenőrzését és hibás bemeneti adatok kezelését.

Az informatikai rendszer üzemeltetése során biztosítani kell a kezelt adatok, információk rendszeres biztonsági mentését. Rendszeres visszaállítási teszteket kell végezni és mindezeket dokumentálni kell.

A Hivatalnál és szervezeteinél megfelelő eljárásokat kell kidolgozni az adathordozók kezelésére, tárolására, nyilvántartására, annak rendszeres, naprakész aktualizálására, valamint ezek megsemmisüléstől és illetéktelen hozzáféréstől történő védelmére. Az eljárások kidolgozásának célja, az ügymenet folytonosságának fenntartása és a szervezet vagyonának megóvása.

Az adathordozók elhelyezése során biztosítani kell, hogy az elhelyezés feltételei megfeleljenek az adatok, információk biztonsági osztályba sorolási modelljében meghatározott követelményeknek.

e) Szoftverkezelés biztonságánál a Hivatal és szervezetei informatikai rendszereiben kizárólag jogtiszta, az üzemeltetéshez, adatfeldolgozáshoz szükséges, engedélyezett alapprogramok, irodai szoftvercsomagok és feldolgozó programok futtathatók.

f) Rosszindulatú szoftverek elleni védekezés

A szoftverek és informatikai rendszerek sebezhetőek a rendszerbe bejutó rosszindulatú szoftverek (vírusok, trójai falovak) által.

A rossz szándékú szoftverek kártételeinek megelőzésre megfelelő megelőző, észlelési és korrekciós mechanizmusokat kell alkalmazni.

3.2.3 Egyéb feladatok tekintetében

a) A folyamatos működés biztosítása

A folyamatos működés tervezésének és biztosításának célja, hogy az ügymenet tevékenységében bekövetkezett zavarokat ellensúlyozni lehessen és a kritikus folyamatok védettek legyenek a nagyobb hibák és katasztrófák következményeitől (üzletmenet-folytonosság).

Le kell vonni a bekövetkezett katasztrófák következményeit, vizsgálni kell a szolgáltatások kiesését és a biztonság sérülését.

b) Informatikai biztonsági események észlelése és kezelése

A Hivatalnak és szervezeteinek érdeke, hogy a szervezet informatikai biztonságáért felelős vezetői mielőbb értesüljenek a bekövetkezett biztonsági eseményekről. Minden alkalmazottnak (külső vagy belső) ismernie kell azt az eljárást, amelyben jelenthetik az általuk felismert biztonsági eseményeket.

Informatikai biztonsági esemény bekövetkezésekor, arról a közvetlen munkahelyi vezetőt és az informatikusokat kell értesíteni és foganatosítani kell a megfelelő válaszintézkedéseket.

Az informatikai biztonság terén a védekezés szempontjából fontos, hogy a korábban történt informatikai biztonsági eseményeket időben visszamenőleg tételesen, minden technikai körülményükkel együtt fel lehessen dolgozni (naplózás).

c) Rendszerfejlesztések biztonsági követelményei

A rendszerek biztonsági követelményeinek meghatározása során, rendszer alatt értjük az infrastrukturális elemeket, objektumokat, alkalmazásokat stb. Biztonsági szempontból

kiemelkedő, hogy a biztonság, mint kritérium jelen legyen az alkalmazások és szolgáltatások tervezésétől kezdődően az ügymenet folyamataiba történő implementálásig.

Kelt: 2021.01.18.

Zelenka Andrea sk.

jegyző