Országos Atomenergia Hivatal

Informatikai biztonságpolitika

Az informatikai biztonság az elektronikus információs rendszer olyan állapota, amikor a védelem az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Az Országos Atomenergia Hivatal (a továbbiakban: Hivatal) vezetésének meggyőződése, hogy a Hivatal által kezelt adatok és információk az atomenergia békés célú felhasználásának biztonsága érdekében a különböző fenyegetések ellen meg kell védeni. Az Hivatal vezetése biztosítja a teljesítéshez szükséges feltételeket és erőforrásokat.

Az informatikai biztonságpolitika a Hivatal vezetésének akaratnyilvánítása a szervezet informatikai rendszereinek és azok által kezelt adat- és információvagyon bizalmasságának, sértetlenségének, valamint rendelkezésre állásának megőrzésére és fenntartására irányuló intézkedések bevezetésére, fenntartására.

Jelen politika célja az alapelvek és célkitűzések meghatározása, amelyek az informatikai biztonsági döntések meghozatalában kiemelt szempontokat képviselnek az alacsonyabb szintű szabályozási eszközök (Informatikai Biztonsági Stratégia, Informatikai Biztonsági Szabályzat, egyéb informatikai tárgyú belső szabályozó dokumentumok) kialakítása és bevezetése során.

Az informatikai biztonságpolitika személyi hatálya kiterjed

- a Hivatal minden munkatársára,
- a Hivatal tevékenységeinek ellátásában résztvevő, szerződéses jogviszonyban álló külső partnerekre,
- a Hivatal informatikai fejlesztését végző, üzemeltetését támogató, szerződéses viszonyban tevékenykedő partnereire.

A személyi hatály alá tartozóknak ismerniük és követniük kell a jelen politika célkitűzéseit. A hivatallal szerződéses kapcsolatban álló partnerekre az informatikai biztonságpolitika érvényesülését a szerződés tartalmának megfelelő kialakításával kell biztosítani.

ALAPELVEK

Az informatikai biztonsági tevékenységek tekintetében a Hivatal:

- átfogó, az egész szervezetre kiterjedő irányítással és a megfelelő erőforrásokkal kell rendelkezzen,
- lehetővé kell tegye a költséghatékony és következetes kockázatkezelési folyamatok végrehajtását az egész szervezetben,
- az egyes védelmi intézkedések a felmerülő kockázatokkal arányos kialakítását,
- a védelmi intézkedések kiválasztása, megvalósítása, folyamatos felügyelete egy szisztematikus, strukturált és átlátható folyamatként alakítja ki és építi be a szervezeti működésbe.

Kockázatarányosság

A védelem mértéke és költségei arányosak legyenek a felmért kockázatokkal, a védelem kialakításánál az ésszerűen elérhető legkisebb kockázatra kell törekedni. A hivatal vezetése célul tűzte ki az ésszerű kockázatokkal arányos védelem érdekében a kockázatelemzés belső

szabályozását, végrehajtását, továbbá a kockázatelemzés eredményeinek beépítését az informatikai biztonsági védelembe.
A kockázatkezelési feladatoknak a célja végső soron az, hogy biztosítsák a szükséges információkat és erőforrásokat a szervezet céljait érintő, a rendszerek üzemeltetéséből és használatából eredő információbiztonsági/kiberbiztonsági kockázatok sikeres kezeléséhez. A felkészülési lépések támogatják az erőforrások azonosítását, rangsorolását, a szervezeti kommunikációt, a védelmi intézkedések hatékonyabb kialakítását. Következetes végrehajtásuk csökkentheti a rendszerfejlesztés és a vagyonvédelem költségeit.

Teljeskörűség
Az informatikai védelem teljeskörűsége azt jelenti, hogy a hivatal

- informatikai rendszerének összes rendszerelemére,
- az informatikai rendszerek teljes számítástechnikai infrastruktúrájára és összes alkalmazására,
- mind a központi, mind a végponti informatikai eszközökre és környezetükre egyaránt érvényesül a védelem, mind az adminisztratív, a fizikai és a logikai védelem területén.

A védelem zártsága
A zárt védelem akkor biztosított, ha megvalósításra kerültek a kockázatelemzés során feltárt összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések, mind az adminisztratív, a fizikai és a logikai védelem területén, és azok szerves egységet alkotnak.

A védelem folytonossága
Az informatikai rendszerek bevezetése során kialakított védelmi képességeket a rendszer teljes életciklusa alatt folyamatosan biztosítani és fejleszteni kell.

CÉLKITŰZÉSEK

Hitelesség
A Hivatal vezetésének célja a hivatal kezelésében lévő adatok és információk hitelességnek biztosítása. Minden kétséget kizáróan megállapítható kell legyen a Hivatal informatikai rendszereibe bekerülő, azokban tárolt adat és információ forrása, az adat és információ valóságnak való megfelelősége, továbbá biztosítani kell, hogy a feldolgozás, felhasználás és tárolás során megőrizze minőségét.

Bizalmasság
A hivatal vezetésének célja, hogy a Hivatal által kezelt adatokhoz és információkhoz való hozzáférés tekintetében a bizalmasságot fenn kell tartani, azaz az adatokhoz és információkhoz csak az arra feljogosítottak férhessenek hozzá. A bizalmasság érvényesülését elsősorban az informatikai rendszerben történő adathozzáférések és adatkezelés, valamint a hivatal kommunikációja során kell biztosítani.

Sértetlenség
A Hivatal vezetésének célja a sértetlenség biztosítása a hivatal adatkezelése, adatfeldolgozása és közzététele során. A Hivatal által történő adatkezelés során követelmény, hogy pontos és a valóságnak mindenben megfelelő információk kerüljenek a rendszerben feldolgozásra, és ezen információk sértetlensége az adatkezelés, adatfeldolgozás és során mindvégig biztosított legyen.

Rendelkezésre állás
A Hivatal vezetésének célja a Hivatal által kezelt adatok és információk rendelkezésre állásának biztosítása. A Hivatalba beérkező, feldolgozott, tárolt információk tekintetében biztosítani kell azok gyors visszakereshetőségét az informatikai rendszerek funkcióinak és elérhetőségének folyamatos biztosításával.

A célkitűzések teljesülése érdekében:

- A Hivatal az információvédelem területén biztosítja az informatikai rendszerelemek gyártói ajánlásoknak és biztonsági követelményeknek történő megfelelését.
- A Hivatal a rendszer alkalmazására és üzemeltetésére vonatkozó szervezeti és működési rendeket, nyilvántartási és tájékoztatási szabályokat, az informatika alkalmazásából eredő biztonsági kockázatok figyelembevételével úgy alakítja ki, hogy a felelősségi körök és az egyértelmű személyes felelősségek meghatározhatók legyenek.
- A Hivatal biztosítja a rendszer üzemeltetése szempontjából összeférhetetlen szerep- és feladatkörök szétválasztását mind szervezeti, mind személyi tekintetben.
- A Hivatal a rendszert a vonatkozó Európai Uniós és hazai jogszabályoknak, valamint szakmai sztenderdeknek és legjobb gyakorlatnak megfelelően alakítja ki és üzemelteti, továbbá rendszeres időközönként felülvizsgálja.
- Az elektronikus információs rendszereket érintő fenyegetések megfelelő kezeléséhez a jogszabályi környezet[1] által előírt kiberbiztonsági követelményekkel le kell fedni a rendszerek teljes életciklusát, támogatni kell a kiberbiztonsági kockázatkezelés szervezeti kereteinek kialakítását, meg kell határozniuk a védelmi intézkedésekkel kapcsolatos elvárásokat, valamint biztosítani kell azok teljesülésének folyamatos felügyeletét.
- A Hivatal az ügymenet folyamatosságát menedzselő folyamatokat és hiba/katasztrófatűrő infrastruktúrát hoz létre annak érdekében, hogy megelőző és helyreállító funkciók alkalmazásával minimalizálja az üzemszerű működés katasztrófák és egyéb rendkívüli események hatására előálló kimaradásának idejét.
- A Hivatal éves rendszerességgel vagy az informatikai rendszerében történt nagyobb változás esetén ellenőrzi és felülvizsgálja a rendszer elemeinek és műszaki környezetének információbiztonsági szintjét és állapotát. A felülvizsgálat eredményének ismeretében haladéktalanul megteszi a szükség szerinti intézkedéseket.
- A hatályos informatikai biztonsági előírásokat a Hivatal felhasználói számára elérhetővé teszi és azokat rendszeres oktatások formájában tudatosítja.

Budapest, 2025. február 25.

Kádár Andrea Beatrix, sk.

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről
7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről