

Informatikai biztonságpolitika

Az informatikai biztonság az elektronikus információs rendszer olyan állapota, amikor a védelem az elektronikus információs rendszerben kezelt adatok 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 OAH vezetésének meggyőződése, hogy az OAH által kezelt információk az állampolgárok olyan vagyona, amelyet az atomenergia békés célú felhasználásának biztonsága érdekében a különböző fenyegetések ellen meg kell védeni. Az OAH vezetése biztosítja a teljesítéshez szükséges feltételeket és erőforrásokat.

Az informatikai biztonságpolitika a hivatal vezetésének akaratnyilvánítása a szervezet informatikai rendszereinek és azok által kezelt információvagyon bizalmasságának, sértetlenségének, valamint rendelkezésre állásának megőrzésére és fenntartására irányuló intézkedések bevezetésére. Jelen politika alapul szolgál az alacsonyabb szintű szabályozási eszközök (Informatikai Biztonsági Stratégia, Informatikai Biztonsági Szabályzat, egyéb informatikai tárgyú eljárásrendek) kialakítására és bevezetésére.

Az informatikai biztonságpolitika személyi hatálya kiterjed

- a hivatal minden munkatársára,
- a hivatal tevékenységeinek ellátását segítő külső partnerekre,
- a hivatal informatikai üzemeltetést, fejlesztést végző szerződéses viszonyban tevékenykedő partnereire.

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

ALAPELVEK

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.

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 folytonosan biztosítani és fejleszteni kell.

CÉLKITŰZÉSEK

Hitelesség

A hivatal vezetésének célja a hivatal kezelésében lévő adatok hitelességnek biztosítása. Minden kétséget kizáróan megállapítható kell legyen a hivatal informatikai rendszereibe bekerülő, azokban tárolt adat forrása, az adat 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 való hozzáférés tekintetében a bizalmasságot fenn kell tartani, azaz az adatokhoz 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 kommunikációja 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 során mindvégig biztosított legyen.

Rendelkezésre állás

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

Budapest, 2017. november 6.

