

INFORMÁCIÓBIZTONSÁGI POLITIKA

A Paks II. Atomerőmű Zrt. (a továbbiakban Társaság), az új paksi telephelyű atomerőművi blokkok létesítésének lebonyolítására, végrehajtására, valamint a szükséges előzetes engedélyek beszerzésére, a beruházás lebonyolítására majd az új blokkok üzemeltetésére alapított projektársaság. Az Információbiztonsági Politika (a továbbiakban: IBP) a Társaság vezetőségének szándéknyilvánítása a szervezet által kezelt információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetésére.

Az IBP és kapcsolódó szabályozó dokumentumai meghatározzák azokat az alapelveket, amelyek mentén a Társaság kialakítja és biztosítja az Információbiztonság érvényre juttatásához szükséges feltételeket, működési gyakorlatokat.

Az IBP személyi hatálya kiterjed a Társaság valamennyi munkavállalójára, akik felhasználják, feldolgozzák, illetve felügyelik és ellenőrzik a keletkező, illetve felhasznált adatokat, információkat.

Az IBP tárgyi hatálya kiterjed a Társaság által használt valamennyi adathordozóra, alkalmazásra, alapszoftverre, hardver elemre, környezeti infrastruktúra elemre és objektumra.

Az IBP területi hatálya kiterjed a Társaság valamennyi saját, és mindenkor bérelt helyiségeire, a társasági munkavállaló home office vagy távmunka munkavégzés helyére, a kiszervezett adatfeldolgozási- és üzemeltetési tevékenységeinek külső helyszíneire, továbbá a nem munkahelyen történő használatra kiadott eszközökre egyaránt.

A Társaság vezetősége elvárja, hogy mindenki, aki a Társaság adatvagyonába tartozó adatokat kezel, azokkal munkát végez, annak során a biztonságért felelős magatartást tanúsítson, cselekedeteivel és döntéseivel is fenntartsa és erősítse a biztonságot, továbbá legyen felkészült arra is, hogy az uralkodó gyakorlatot kétségbe vonja, és erről a közvetlen vezetőjét haladéktalanul tájékoztassa, ha úgy ítéli meg, hogy az az információbiztonságot veszélyezteti.

Az IBP alapelvei közé tartoznak:

- A védelem teljeskörűségének alapelve
- A védelem zártságának alapelve
- A védelem kockázatarányosságának alapelve
- A védelem folytonosságának alapelve

A Társaság vezetősége célul tűzte ki – a kockázatokkal arányos védelem biztosítása érdekében – kockázatelemzés rendszeres, belső szabályozás szerinti elvégzését a fenyegetések, a gyenge pontok, a nem elviselhető kockázatú tényezők meghatározására, valamint az ezek alapján kialakítandó védelmi intézkedések végrehajtására.

A Társaság vezetősége elkötelezett amellett, hogy az információbiztonság jó gyakorlatait folyamatosan figyelemmel kíséri, azok alkalmazását bevezeti. Az információbiztonsági incidenseket haladéktalanul kivizsgálja, majd a végrehajtott helyesbítő, megelőző intézkedésről megfelelő módon tájékoztatja az adatvagyon elemeket felhasználó munkavállalóit.

Az IBP-t a Társaság illetékes biztonságért felelős szervezeti egysége rendszeres időközönként felülvizsgálja.

Paks, 2024.02.02

Jákli Gergely