# INFORMATIKAI BIZTONSÁGI 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 projekttársaság. Az Informatikai Biztonsági Politika (a továbbiakban: IBP) a Társaság legfelső vezetésének szándéknyilvánítása a szervezet informatikai rendszerei 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 Informatikai Biztonság érvényre juttatásához szükséges feltételeket, működési gyakorlatokat.
Az IBP személyi hatálya kiterjed a Társaság valamennyi munkavállalójára, továbbá a Társaság által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi 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 székhelyére, telephelyeire és fióktelepére és valamennyi, mindenkor bérelt helyiségeire, a kiszervezett adatfeldolgozási- és üzemeltetési tevékenységeinek külső helyszíneire, továbbá a nem munkahelyen történő használatra kiadott eszközökre egyaránt.

A Társaság vezetése elvárja, hogy mindenki, aki a Társaság által biztosított informatikai eszközökön dolgozik, 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 a biztonságot veszélyezteti.

Az IBP alapelvei közé tartoznak:

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

A Társaság 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 meghatározása, valamint az ezek alapján kialakítandó védelmi intézkedésekre.

A Társaság elkötelezett amellett, hogy az informatikai biztonság jó gyakorlatait folyamatosan figyelemmel kíséri, azok alkalmazását bevezeti. Az informatikai biztonsági incidenseket haladéktalanul kivizsgálja, majd a végrehajtott helyesbítő, megelőző intézkedésről megfelelő módon tájékoztatja az informatikai eszközöket használó munkavállalóit.
Az IBP-t a Társaság illetékes biztonságért felelős szervezete rendszeres időközönként felülvizsgálja.

Paks, 2021. április 29.

Lenkei István
vezérigazgató