INFORMATION SECURITY POLICY

Paks II NPP Ltd. (hereinafter: the Company) is a project company established to manage and implement the construction of the new nuclear power plant units at the Paks site, to obtain the necessary preliminary licenses, to implement the project, and subsequently to operate the new units. The Information Security Policy (hereinafter: ISP) represents the declaration of intent of the Company's management to introduce measures aimed at preserving and maintaining the confidentiality, authenticity, integrity, availability, and functionality of the information assets handled by the organization.
The ISP and its related regulating documents define the principles under which the Company establishes and ensures the conditions and operational practices necessary for the effective enforcement of Information Security.
The personal scope of the ISP extends to all employees of the Company who use, process, supervise, or control the data and information generated or used.
The material scope of the ISP covers all data carriers, applications, system software, hardware elements, environmental infrastructure elements, and facilities used by the Company.
The territorial scope of the ISP extends to all premises owned or leased by the Company, to the home office or remote workstations of the Company's employees, to the external locations of outsourced data processing and operations, and to devices issued for use outside the workplace.

The Company's management expects all individuals who handle and work with the Company's data assets to demonstrate responsible behavior with regard to security, uphold and strengthen security through their actions and decisions, and be prepared to challenge prevailing practices. They shall inform their line manager immediately if they consider that such practices endanger information security.

The fundamental principles of the ISP include:

- The principle of comprehensive protection
- The principle of closed protection
- The principle of risk-proportionate protection
- The principle of continuity of protection

The Company's management has set the objective of ensuring protection proportionate to risks by regularly conducting risk analyses in accordance with internal regulations to identify threats, vulnerabilities, and unacceptable risk factors, and to implement protective measures based on these findings.
The Company's management is committed to continuously monitoring and implementing the best practices in information security. Information security incidents are investigated without delay, and employees using information assets are informed of the corrective and preventive measures implemented.

The ISP is reviewed at regular intervals by the competent organizational unit responsible for security within the Company.

Paks, 02.02.2024

Jákli Gergely
2024-02-02

Gergely Jákli